

Exhibit 7

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Gregory G. Raleigh et al. Attorney Docket No.: 39843-0183IP2
U.S. Patent No.: 9,609,510
Issue Date: March 28, 2017
Appl. Serial No.: 14/208,236
Filing Date: March 13, 2014
Title: AUTOMATED CREDENTIAL PORTING FOR MOBILE
DEVICES

Mail Stop Patent Board

Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR *INTER PARTES* REVIEW OF
UNITED STATES PATENT NO. 9,609,510
PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42

TABLE OF CONTENTS

I.	REQUIREMENTS FOR IPR	1
A.	Grounds for Standing.....	1
B.	Challenge and Relief Requested.....	1
II.	SUMMARY OF THE '510 PATENT	3
A.	Brief Description.....	3
B.	Prosecution History.....	5
III.	LEVEL OF ORDINARY SKILL	5
IV.	CLAIM CONSTRUCTION	6
V.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	7
A.	GROUND 1A: Salmela in view of Rishy-Maharaj render obvious the limitations of the Challenged Claims recited in claims 1, 2, 7, and 38	7
1.	<i>Salmela</i>	<i>7</i>
2.	<i>Rishy-Maharaj.....</i>	<i>10</i>
3.	<i>The Salmela-Rishy-Maharaj Combination</i>	<i>11</i>
4.	<i>Application to Base Limitations of Challenged Claims</i>	<i>14</i>
B.	GROUND 1B: Salmela, in view of Rishy-Maharaj, and further in view of Bennett would have rendered obvious claims 21, 23, and 25	44
1.	<i>Bennett.....</i>	<i>44</i>
2.	<i>The Salmela-Rishy-Maharaj-Bennett Combination</i>	<i>45</i>
3.	<i>Application to Challenged Claims</i>	<i>47</i>
C.	GROUND 1C: Salmela, in view of Rishy-Maharaj, further in view of Bennett, and further in view of FCCReg would have rendered obvious claims 26 and 27	49
1.	<i>FCCReg</i>	<i>49</i>
2.	<i>The Salmela-Rishy-Maharaj-Bennett-FCCReg Combination</i>	<i>50</i>
3.	<i>Application to Challenged Claims</i>	<i>51</i>
D.	GROUND 1D: Salmela, in view of Rishy-Maharaj, and further in view of Ionescu would have rendered obvious claims 12, 13.....	53
1.	<i>Ionescu.....</i>	<i>53</i>
2.	<i>The Salmela-Rishy-Maharaj-Ionescu Combination.....</i>	<i>54</i>
3.	<i>Application to Challenged Claims</i>	<i>57</i>
E.	GROUND 1E: Salmela, in view of Rishy-Maharaj, and further in view of Sigmund would have rendered obvious claims 4, 5, 8-10	57
1.	<i>Sigmund</i>	<i>57</i>
2.	<i>The Salmela-Rishy-Maharaj-Sigmund Combination</i>	<i>58</i>
3.	<i>Application to Challenged Claims</i>	<i>60</i>

F.	GROUND 1F: Salmela, in view of Rishy-Maharaj, and further in view of Johansson would have rendered obvious claim 40	64
1.	<i>Johansson</i>	64
2.	<i>The Salmela-Rishy-Maharaj-Johansson Combination</i>	65
3.	<i>Application to Challenged Claims</i>	67
G.	GROUND 1G: Salmela, in view of Rishy-Maharaj, and further in view of Slavov would have rendered obvious claim 34.....	69
1.	<i>Slavov</i>	69
2.	<i>The Salmela-Rishy-Maharaj-Slavov Combination</i>	69
3.	<i>Application to Challenged Claims</i>	71
H.	GROUND 1H: Salmela, in view of Rishy-Maharaj, and further in view of Gupta would have rendered obvious claim 44	73
1.	<i>Gupta</i>	73
2.	<i>The Salmela-Rishy-Maharaj-Gupta Combination</i>	73
3.	<i>Application to Challenged Claims</i>	74
VI.	PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION.....	75
A.	Discretionary denial under §325(d) is not warranted	75
B.	Discretionary denial under §314(a) is not warranted	76
VII.	CONCLUSION AND FEES	78
VIII.	MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1).....	78
A.	Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1).....	78
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2)	78
C.	Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3).....	79
D.	Service Information	79

LIST OF EXHIBITS

EX1001	U.S. Patent No. 9,609,510 to Raleigh (“the ’510 Patent”)
EX1002	Excerpts from the Prosecution History of the ’510 Patent (“the Prosecution History”)
EX1003	Expert Declaration and Curriculum Vitae of Patrick Traynor, Ph.D.
EX1004	U.S. Publication No. 2009/0217364 (“Salmela”)
EX1005	U.S. Publication No. 2013/0165075 (“Rishy-Maharaj”)
EX1006	U.S. Publication No. 2010/0029273 (“Bennett”)
EX1007	U.S. Publication No. 2012/0236760 (“Ionescu”)
EX1008	U.S. Publication No. 2010/0222024 (“Sigmund”)
EX1009	U.S. Publication No. 2010/0177663 (“Johansson”)
EX1010	U.S. Patent No. 9,191,394 (“Novak”)
EX1011	U.S. Publication No. 2009/0253409 (“Slavov”)
EX1012	Federal Communications Commission (FCC) Regulation (2010), <i>available at</i> , https://www.govinfo.gov/content/pkg/FR-2010-06-22/pdf/2010-15073.pdf (“FCCReg”)
EX1013	U.S. Publication No. 2011/0130119 (“Gupta”)
EX1014	U.S. Publication No. 2008/0122796 (“Jobs”)
EX1015	Samsung Galaxy SII Mobile Phone User Manual (2011), <i>available at</i> https://ringtones.specialtyansweringservice.net/wp-content/uploads/2014/08/manuals/samsung-galaxys2-userguide.pdf

- EX1016 iPhone User Guide For iPhone OS 3.1 Software (2009),
available at
https://cdsassets.apple.com/live/6GJYWVAV/user/ma616_iphone_ios3_1_user_guide.pdf
- EX1017 Architecture and Enablers for Optimized Radio Resource Usage in Heterogeneous Wireless Access Networks (2009), *available at*
https://www.researchgate.net/publication/224371987_Architecture_and_Enablers_for_Optimized_Radio_Resource_Usage_in_Heterogeneous_Wireless_Access_Networks_The_IEEE_19004_Working_Group
- EX1018 Characterizing Radio Resource Allocation for 3G Networks (2010), *available at*
https://www.cs.columbia.edu/~lierranli/coms6998-7Spring2014/papers/RRC3G_imc2010.pdf
- EX1019 Operating System Implications of Fast, Cheap, Non-Volatile Memory (2011), *available at*
https://www.usenix.org/legacy/events/hotos11/tech/final_files/Bailey.pdf
- EX1020 iPod touch User Guide for iOS 5.1 Software (2012), *available at*
https://cdsassets.apple.com/live/6GJYWVAV/user/ma1627_ipod_touch_ios5_user_guide.pdf
- EX1021 Samsung Galaxy SIII 4G LTE Smartphone User Manual (2013), *available at*
https://downloadcenter.samsung.com/content/UM/202101/20210101045744723/ATT_SGH-I747_Galaxy_SIII_English_User_Manual_KK_NE4_F1.pdf
- EX1022 U.S. Publication No. 2009/0249247 (“Tseng”)
- EX1023 U.S. Patent No. 7,280,818 (“Clayton”)
- EX1024 U.S. Patent No. 8,923,824 (“Masterman”)

EX1025	RESERVED
EX1026	Samsung's Stipulation Regarding Invalidity Grounds in Co-Pending District Court Litigation
EX1027	Jacob et al., <i>Memory Systems: Cache, DRAM, Disk</i> (2007) ("Jacob")
EX1028	U.S. Publication No. 2012/0185636 ("Leon")
EX1029	U.S. Patent No. 8,060,748 ("Johansson-748")
EX1030	U.S. Publication No. 2006/0258289 ("Dua")
EX1031	European Telecommunications Standards Institute (ETSI) Technical Specification 23.003 v8.11.0 (2011), <i>available at</i> https://www.etsi.org/deliver/etsi_ts/123000_123099/123003/08.11.00_60/ts_123003v081100p.pdf
EX1032	Control Servers in the Core Network (2000), <i>available at</i> https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=1247211968f9167dbc5e7ea896bd910762e57ba7
EX1033	Wireless Application Protocol (WAP) Architectural Overview (2001), <i>available at</i> https://www.openmobilealliance.org/release/Push/V2_1-20051122-C/WAP-250-PushArchOverview-20010703-a.pdf
EX1034-1099	RESERVED
EX1100	Complaint for Patent Infringement in <i>Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.</i> , 2-24-cv-00228 (EDTX) (Apr. 03, 2024)
EX1101	Memorandum, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings, June 21, 2022, <i>available at</i> https://www.uspto.gov/sites/default/files/documents/interim_pr

Attorney Docket No. 39843-0183IP2

IPR of U.S. Patent No. 9,609,510

[oc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf](#)

EX1102 Docket Control Order in *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.*, Case No. 2:24-cv-00228 (EDTX) (Aug. 9, 2024)

EX1103 Disclosure of Asserted Claims and Infringement Contentions in *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.*, 2-24-cv-00228 (EDTX) (Jul. 11, 2024)

LIST OF CHALLENGED CLAIM ELEMENTS

Claim 1	
[1pre]	A wireless device, comprising:
[1a]	a user interface;
[1b]	memory configured to store:
[1c]	one or more credentials associated with the wireless device, the one or more credentials for authorizing the wireless device to use a wireless access network to access one or more services, and
[1d]	a target credential; and
[1e]	one or more processors configured to execute one or more machine-executable instructions that, when executed by the one or more processors, cause the one or more processors to:
[1f]	obtain, through the user interface, an indication of a user request to replace a particular credential of the one or more credentials with the target credential,
[1g]	detect a network-provisioning state change, and based on the detected network-provisioning state change, automatically
[1h]	determine that the particular credential does not match the target credential,
[1i]	initiate a programming session with a network element communicatively coupled to the wireless device over the wireless access network,
[1j]	obtain an updated credential from the network element, and
[1k]	assist in storing, in memory, the updated credential as the particular credential.
Claim 2	

[2]	The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to: determine that the updated credential does not match the target credential, and based on the determination that the updated credential does not match the target credential, take an action.
Claim 4	
[4]	The wireless device recited in claim 2, wherein the action is to cause a notification to be presented through the user interface, wherein the notification reports an error.
Claim 5	
[5]	The wireless device recited in claim 2, wherein the action is to cause a notification to be presented through the user interface, wherein the notification reports that a procedure is in progress or has not been completed.
Claim 7	
[7]	The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to: determine that the updated credential matches the target credential, and based on the determination that the updated credential matches the target credential, take an action.
Claim 8	
[8]	The wireless device recited in claim 7, wherein the action is to cause a notification to be presented through the user interface, wherein the notification reports that the particular credential has been replaced by the target credential.
Claim 9	
[9]	The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to cause a notification to be presented through the user interface, the

	notification providing information about a status of the user request to replace the particular credential of the one or more credentials with the target credential.
Claim 10	
[10]	The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to cause a notification to be presented through the user interface, the notification requesting confirmation of the user request to replace the particular credential with the target credential.
Claim 12	
[12]	The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that an attempt by the wireless device to place a voice call has failed.
Claim 13	
[13]	The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that an attempt by the wireless device to send a text message has failed.
Claim 21	
[21]	The wireless device recited in claim 1, wherein the one or more credentials comprise a phone number.
Claim 23	
[23]	The wireless device recited in claim 1, wherein the target credential comprises a phone number.
Claim 25	
[25]	The wireless device recited in claim 1, wherein the particular credential comprises a first phone number currently associated with the wireless device, and wherein the target credential comprises a second phone number.

Claim 26	
[26]	The wireless device recited in claim 25, wherein the wireless device is a first wireless device, and wherein the second phone number is, prior to the user request to replace the particular credential with the target credential, associated with a second wireless device.
Claim 27	
[27]	The wireless device recited in claim 25, wherein the second phone number is, prior to the user request to replace the particular credential with the target credential, associated with a land line.
Claim 34	
[34]	The wireless device recited in claim 1, wherein obtaining the indication of the user request to replace the particular credential of the one or more credentials with the target credential comprises obtaining information from a website.
Claim 38	
[38]	The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises contacting the network element using a temporary credential.
Claim 40	
[40]	The wireless device recited in claim 38, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to obtain the temporary credential from a network system communicatively coupled to the wireless device.
Claim 44	
[44]	The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network

Attorney Docket No. 39843-0183IP2

IPR of U.S. Patent No. 9,609,510

	comprises communicating with the network element through a voice call.
--	--

Samsung Electronics Co., Ltd. (“Petitioner” or “Samsung”) petitions for *Inter Partes* Review (“IPR”) of claims 4-5, 8-10, 12-13, 21, 23, 25-27, 34, 40, and 44 (“the Challenged Claims”) of U.S. Patent No. 9,609,510 (“the ’510 Patent”).

I. REQUIREMENTS FOR IPR

A. Grounds for Standing

Petitioner certifies that the ’510 Patent is available for IPR, and Petitioner is not barred or estopped from requesting IPR.

B. Challenge and Relief Requested

Petitioner requests IPR on Grounds 1B-1H listed below:¹

¹ Petitioner has concurrently filed a second petition in IPR2025-00483 challenging claims 1-3, 6-7, 11, 14-25, 28-33, 35-39, 41-43, and 45-48 of the ’510 patent in Ground 1A based on Salmela in view of Rishy-Maharaj. Because the Challenged Claims in this Petition all depend at least in part from independent claim 1, and several Challenged Claims further depend from one of dependent claims 2, 7, or 38, this Petition also includes analysis from Ground 1A that shows how the combined teachings of Salmela and Rishy-Maharaj render obvious all limitations of claims 1, 2, 7, and 38. Petitioner only formally challenges claims 1, 2, 7, and 38 in the IPR2025-00483, however.

<u>Ground</u>	<u>Claims</u>	<u>Basis</u>
1B	21, 23, 25	§103 – Obvious based on Salmela (EX1004), in view of Rishy-Maharaj (EX1005), and further in view of Bennett (EX1006)
1C	26-27	§103 – Obvious based on Salmela, in view of Rishy-Maharaj, further in view of Bennett, and further in view of FCCReg (EX1012)
1D	12-13	§103 – Obvious based on Salmela, in view of Rishy-Maharaj, and further in view of Ionescu (EX1007)
1E	4-5, 8-10	§103 – Obvious based on Salmela, in view of Rishy-Maharaj, and further in view of Sigmund (EX1008)
1F	40	§103 – Obvious based on Salmela, in view of Rishy-Maharaj, and further in view of Johansson (EX1009)
1G	34	§103 – Obvious based on Salmela, in view of Rishy-Maharaj, and further in view of Slavov (EX1011)
1H	44	§103 – Obvious based on Salmela, in view of Rishy-Maharaj, and further in view of Gupta (EX1013)

Grounds 1B-1H are further supported by the expert declaration of Patrick Traynor, Ph.D. (EX1003), and the additional evidence cited herein.

The '510 Patent was filed on March 13, 2014, claiming priority to a provisional application filed on March 14, 2013. Without conceding that the '510 Patent is entitled to the benefit of the provisional application's filing date, Petitioner nonetheless treats March 14, 2013 as the Critical Date of the Challenged Claims for purposes of the analysis in this Petition. Grounds 1B-1H rely on publications that all qualify as prior art under pre-AIA 35 U.S.C. §102 as shown below:

<u>Reference</u>	<u>Filed</u>	<u>Published</u>	<u>Pre-AIA Prior Art Status</u>
Salmela	06/17/2008	08/27/2009	§102(a)-(b), (e)
Rishy-Maharaj	05/23/2012	06/27/2013	§102(e)
Bennett	11/05/2008	02/04/2010	§102(a)-(b), (e)
Ionescu	11/18/2011	09/20/2012	§102(a), (e)
Sigmund	04/25/2008	09/02/2010	§102(a)-(b), (e)
Johansson	06/27/2007	07/15/2010	§102(a)-(b), (e)
Slavov	08/18/2008	10/08/2009	§102(a)-(b), (e)
FCCReg	---	06/22/2010	§102(a)-(b), (e)
Gupta	12/02/2009	06/02/2011	§102(a)-(b), (e)

II. SUMMARY OF THE '510 PATENT

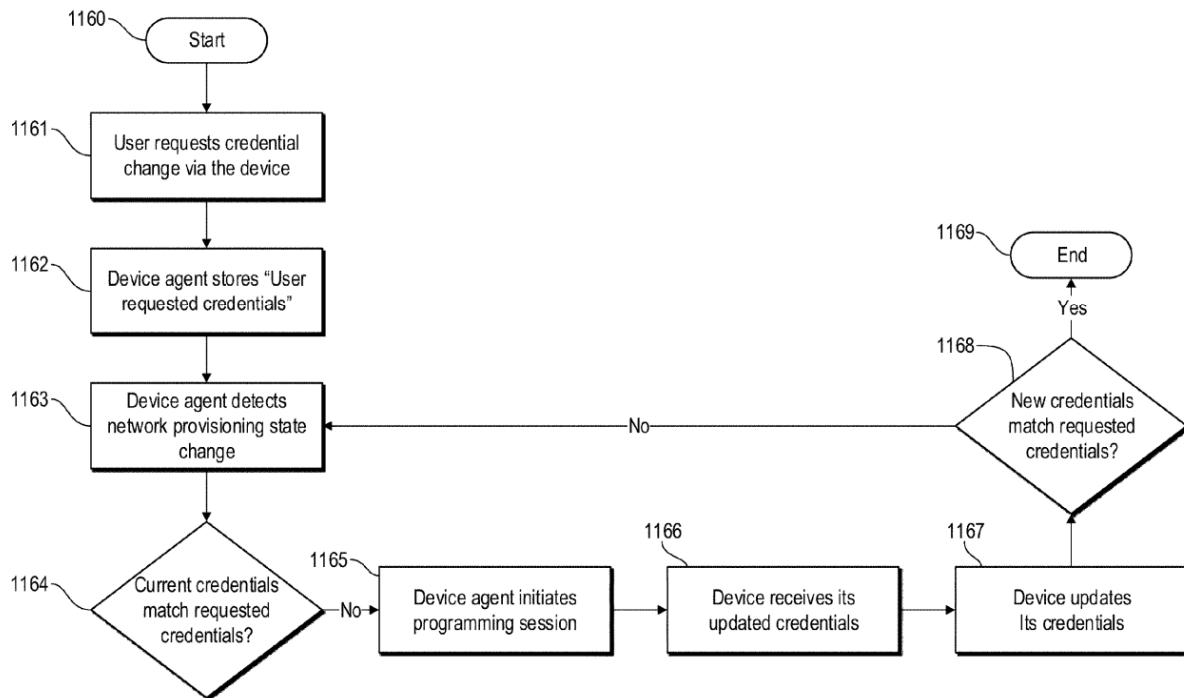
A. Brief Description

The '510 Patent describes techniques for automatically updating network access credentials for a wireless device (e.g., a mobile phone). EX1001, 5:10-6:57, 6:4-7:15, 9:4-10:56, 11:20-12:44; EX1003, ¶24. The credentials can include, for example, an international mobile subscriber identity (IMSI), a phone number, or an internet protocol (IP) address. EX1001, 5:21-48, 9:59-10:8.

In some embodiments, the user submits a request to update the credentials on a wireless device through a user interface of the device. EX1001, 7:28-68, 10:57-67, FIG. 3; EX1003, ¶25. The device can continue to operate on its current (non-updated) credentials for a time while the user's request is processed by a service provider. EX1001, 9:4-35, 10:57-11:27. Eventually, however, the current

credentials will expire or be deactivated by the service provider pursuant to the user's request, and consequently, the device will be unable to gain access to the network using its current credentials. EX1001, 9:4-35, 10:57-11:27. The device can interpret such a failure to access the network with its current credentials as a "network provisioning state change," and in response, the device automatically initiates operations to update its credentials as shown in FIG. 3:

FIG. 3



EX1001, FIG. 3.

As depicted above, the wireless device can perform several actions upon detecting a network provisioning state change. EX1001, 11:38-12:33. These actions can include determining whether the device's current credentials match the

user-requested credentials, initiating a programming session with a network element, receiving updated credentials, and determining whether the updated credentials match the user-requested credentials. EX1001, 11:38-12:33. The '510 Patent explains that credentials can be updated “automatically” and “without informing the subscriber” in some embodiments. EX1001, 12:34-35. Consequently, apart from the initial step of receiving a user request to update credentials, the wireless device can automatically perform the subsequent operations depicted in FIG. 3 to update the device’s credentials without user participation. EX1001, 10:57-12:44; EX1003, ¶26.

B. Prosecution History

The Examiner allowed the claims following Applicant’s response to the first office action. EX1002, 445-447; 450-458; 497-504; EX1003, ¶27-31. Despite this history, the '510 Patent never should have been allowed. As demonstrated by this Petition, the prior art teaches and renders obvious each of the Challenged Claims. EX1003, ¶31.

III. LEVEL OF ORDINARY SKILL

A person of ordinary skill in the art (“POSITA”) for the '510 Patent by the Critical Date (March 14, 2013) would have had a Bachelor’s degree in electrical engineering, computer engineering, computer science, or equivalent, and two years of industry experience in networking security, mobile device communications

security, and/or wireless digital communications systems security. EX1003, ¶21.

Additional education might compensate for less experience, and vice versa.

EX1003, ¶21-22.

IV. CLAIM CONSTRUCTION

Petitioner acknowledges that claim terms in an IPR are construed consistent with the *Phillips* standard applied in district court proceedings. *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005); 37 C.F.R. §42.100. Considering the substantial overlap between the preferred embodiments of the '510 Patent and the prior art combinations advanced in Ground 1A of this Petition, Petitioner submits that no claim terms presently require formal constructions for purposes of resolving controversies in this proceeding. *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011); *Google Inc. v. Intellectual Ventures II LLC*, 701 Fed. Appx. 946, 956 (Fed. Cir. 2017) (“do not require construction” to “resolv[e] the parties’ patentability arguments”); EX1003, ¶23.

Petitioner reserves the right to respond to any constructions offered by Patent Owner or adopted by the Board. Petitioner is not conceding that each Challenged Claim satisfies all statutory requirements, nor is Petitioner waiving any arguments concerning indefiniteness or claim scope that can only be raised in district court or otherwise outside the context of an IPR. *Mylan Pharm. Inc. v. Horizon Pharma USA, Inc.*, IPR2018-00272, Paper 35, 6-8 (PTAB 2019). The Board has regularly

compared indefinite claims to the prior art for purposes of considering unpatentability. *See, e.g., Chicago Mercantile Exchange, Inc. v. 5th Market, Inc.*, CBM2013-00027, Paper 33, 3 (PTAB 2014); *SAP America, Inc. v. Lakshmi Arunachalam*, CBM2013-00013, Paper 61, 29 (PTAB 2014). For this petition, Petitioner applies prior art in a manner consistent with Patent Owner's allegations of infringement before the district court.

V. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. GROUND 1A: Salmela in view of Rishy-Maharaj render obvious the limitations of the Challenged Claims recited in claims 1, 2, 7, and 38

1. Salmela

Like the '510 Patent, Salmela describes techniques for automatically updating credentials on a wireless device. EX1004, [0003]-[0012], [0020]-[0027]; EX1003, ¶23-26. According to Salmela, “[s]ecure and convenient management of subscription credentials [stood] as an ongoing challenge in the field of wireless communications.” EX1004, [0003]. Salmela also explains that “subscription credentials ... link the device to a given network service provider (home operator) and allow it to authenticate itself to the operator's home network, and to any number of visited networks, subject to roaming agreements, etc.” EX1004, [0003]. Recognizing that it is sometimes difficult for device owners to manually update subscription credentials when they “chang[e] subscription plans, and particularly when changing home operator affiliations,” Salmela proposes a credential updating

process that is automatically triggered upon detecting “a failure to gain network access.” EX1004, [0009]; [0027], *generally* [0020]-[0027], FIG. 2.

In Salmela’s process, the wireless device is configured to “revert[] from subscription credentials to temporary access credentials, in response to detecting an access failure.” EX1004, [0010]; EX1003, ¶34. Such network access failure can occur when the device’s current subscription credentials expire or are otherwise no longer valid to authenticate the device on the network under the subscription plan that the device had been operating on previously, which can result from the device owner having changed subscription plans to a new home operator. EX1004, [0010]; EX1003, ¶35. “The device [then] uses [] temporary access credentials to gain temporary network access,” and if “the device determines [that] it needs new subscription credentials,” it “uses the temporary access to obtain them.” EX1004, [0010], *see also*, [0011]-[0013], [0020]-[0028], [0031], FIGS. 1-2, 4. For example, temporary network access allows the device to (1) determine that new subscription credentials are needed, (2) initiate a programming session with a credentialing server if it is determined that new subscription credentials are needed, (3) obtain the new subscription credentials from the credentialing server, and (4) download the new subscription credentials to a secure element in a memory of the device. EX1004, [0024], [0025], [0041].

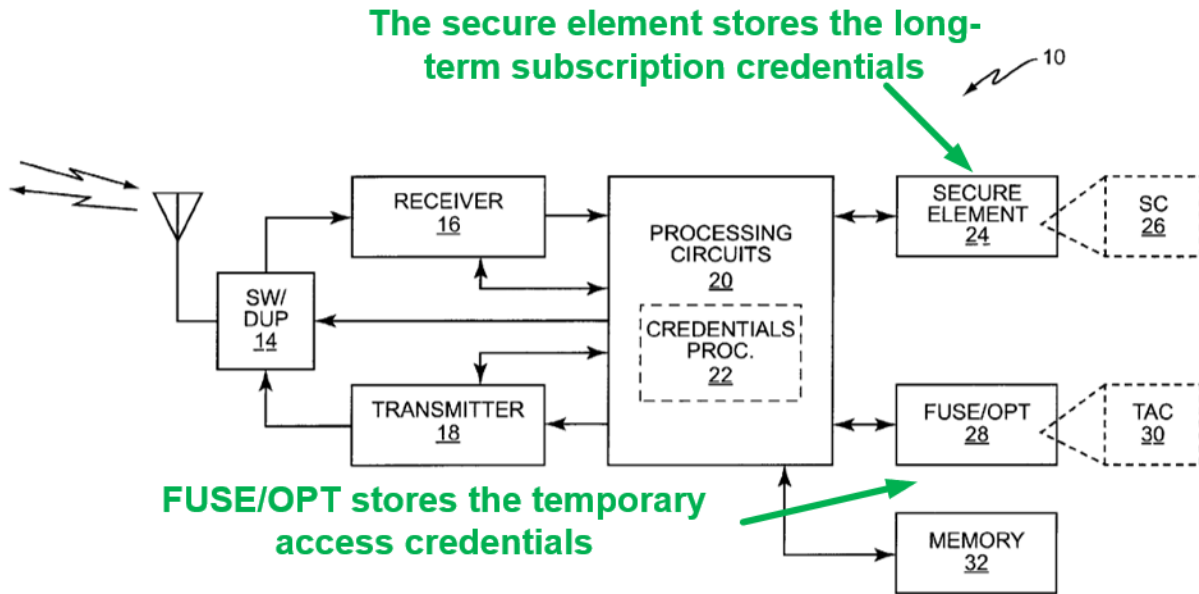


FIG. 1

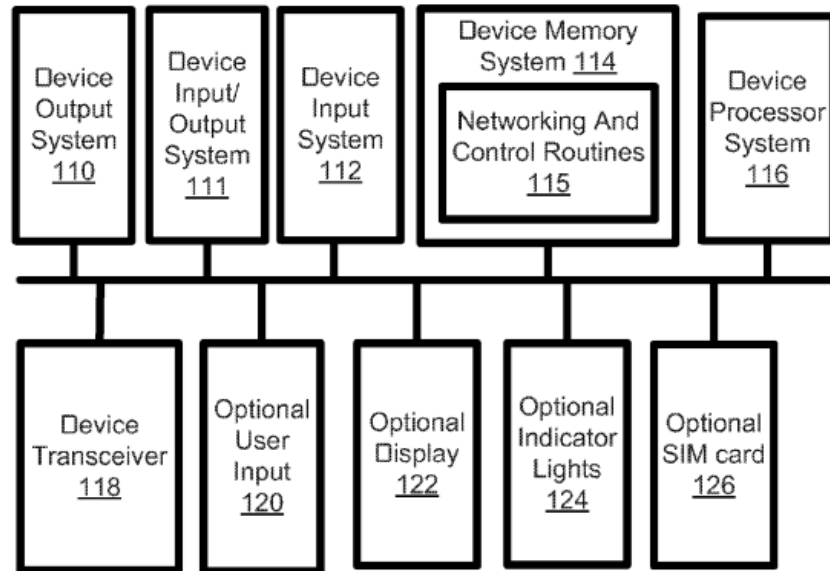
EX1004, FIG. 1.

With this process, Salmela allows “a device owner” to “change subscriptions without having to first update the affected device.” EX1004, [0050]. In particular, when the device owner changes subscriptions, each device associated with the changed subscription automatically updates its own credentials by performing Salmela’s process of detecting network access failure, reverting to temporary credentials, and updating to new credentials associated with the changed subscription. EX1004, [0011] (“To the extent that any subscription agreement change invalidates device-held subscription credentials, each such device will detect access failure with its current subscription credentials and revert to temporary access credentials and contact a registration service or other entity to

determine if new subscription credentials are needed.”), [0024], [0025], [0041]; EX1003, ¶36.

2. *Rishy-Maharaj*

As with Salmela and the ’510 Patent, Rishy-Maharaj describes techniques for updating credentials on a wireless device according to a user-selected subscription plan. EX1004, [0010]-[0012]; EX1005, [0028]-[0036]; EX1003, ¶37. Although Salmela does not describe in detail how the user initiates a request to change subscription plans or the home operator, Rishy-Maharaj explains that the request can be submitted through a user interface of a wireless device. EX1005, [0108]-[0121]. For example, Rishy-Maharaj describes a user interface of a wireless device that “list[s] services...for the user to select” and that allows “the user to select a plan.” EX1005, [0112]; *see also* (“[T]he user may select the subscription plan and network that best suits the user.”). The user interface of the device may include a “device output system,” a “device input system,” an “optional user input,” and an “optional display,” like that depicted below in FIG. 1B:



EX1005, FIG. 1B.

EX1005, [0058]-[0060], [0066], [0067], FIG. 1B.

3. *The Salmela-Rishy-Maharaj Combination*

As discussed above, Salmela discloses that the owner of one or more wireless devices can request to update a subscription plan used by those devices to access the wireless network(s) of an affiliated home operator. EX1004, [0008]-[0011], [0053], Abstract; *supra*, §V.A.1. While Salmela does not expressly describe how the device owner submits a request to update the subscription plan, Rishy-Maharaj demonstrates that one known option was to input the request through a user interface of an affected wireless device. EX1005, [0111]-[0112]; *supra*, §V.A.2; EX1003, ¶38. It would have been obvious to apply Rishy-Maharaj's teachings in this regard to Salmela such that Salmela's device owner would select to activate or change subscriptions through a user interface of a

wireless device, thereby prompting each of the user's devices associated with the selected subscription plan to automatically obtain new subscription credentials as needed upon detecting a failure to gain network access with their current subscription credentials, according to the processes disclosed in Salmela. EX1003, ¶38. A POSITA would have combined the teachings of Salmela and Rishy-Maharaj in this manner for multiple reasons.

First, a POSITA would have recognized that implementing Salmela's wireless device to include a "user interface" (e.g., user input 120) as suggested by Rishy-Maharaj would be advantageous in allowing a user to activate or change subscription plans on the wireless device itself without requiring the user to interact with other devices or with a call center. EX1005, [0058]-[0060], [0066], [0067], FIG. 1B; EX1003, ¶39. This would make the process of activating or changing subscriptions more convenient to the user by reducing the time, burden, and resources that would otherwise be necessary for the user to activate or change subscriptions. EX1005, [0066]; EX1003, ¶39.

Second, implementing Salmela's wireless device to include a "user interface" (e.g., display 122) as suggested by Rishy-Maharaj would allow the wireless device to provide information to the user in a manner that would conveniently guide the user's selection of a subscription plan. EX1005, [0067]; EX1003, ¶40. For example, the wireless device in the Salmela-Rishy-Maharaj

combination can be advantageously “used for displaying information to the user about how to operate wireless device 102, about available local networks, prompts for proceeding through the process of selecting a local network, and/or adding funds to an established subscription.” EX1005, [0067]; EX1003, ¶40. This information displayed by the wireless device would aid the user in selecting a subscription plan on a single device. EX1003, ¶40.

Third, implementing Salmela’s wireless device to include a “user interface” (e.g., display 122) as suggested by Rishy-Maharaj would have been obvious as a predictable application of a known technique (e.g., enabling selection of a subscription plan through a user interface of a wireless device) to a known system as taught by Salmela to achieve merely predictable results. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007) (an alleged invention that “simply arranges old elements with each performing the same function it had been known to perform” is obvious); EX1003, ¶41.

Fourth, it would have been obvious for a POSITA to implement Salmela’s wireless device with a user interface as suggested by Rishy-Maharaj because doing so represents one of a finite number of predictable solutions for receiving a user selection from a user. EX1003, ¶42. A POSITA would have appreciated, for example, that a request to change subscription plans for a wireless device could be made through a user interface of the wireless device itself, using another device, or

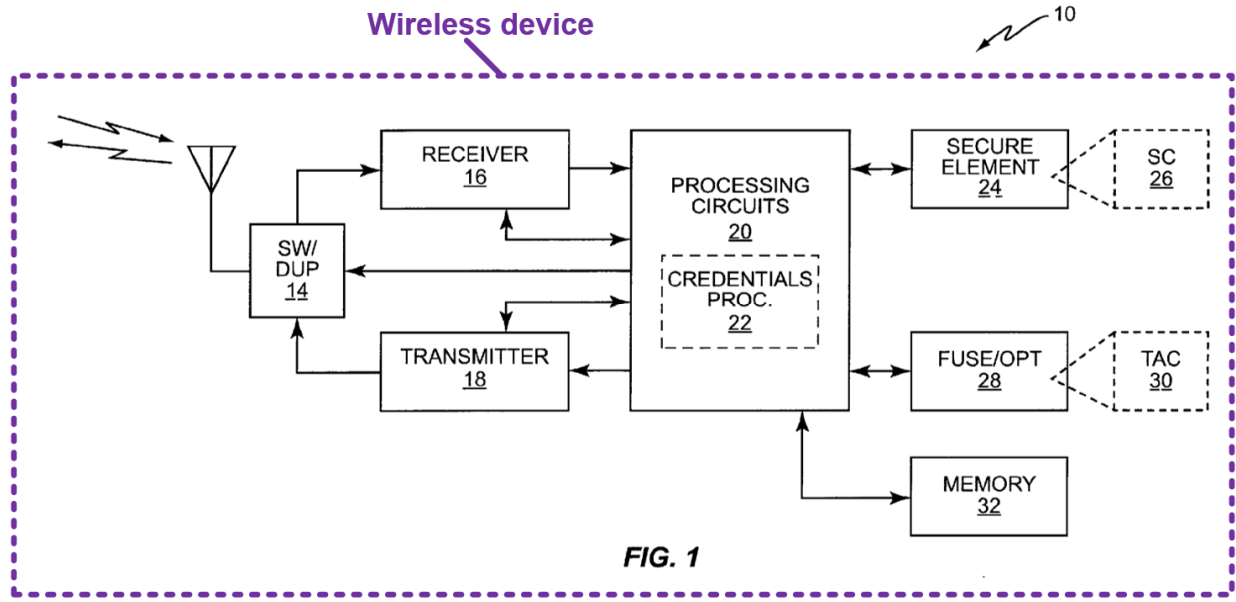
by relaying the request to a third-party (e.g., a call center, retail outlet, or other agent of a network service provider). A POSITA would have been driven toward the first option in many cases for the reasons discussed above, including to promote user convenience in a straightforward manner. EX1003, ¶42.

A POSITA would have reasonably expected success implementing the Salmela-Rishy-Maharaj combination since wireless devices having user interfaces having hardware capable of executing software and performing the functions described above were well known before the Critical Date of the '510 Patent. EX1003, ¶43; *see also* EX1004, [0021], [0030].

4. *Application to Base Limitations of Challenged Claims*

Element [1pre]

To the extent the preamble is a limitation, the Salmela-Rishy-Maharaj combination renders obvious the claimed “wireless device.” EX1003, ¶95. For example, Salmela discloses a **wireless** communication **device** 10. EX1004, [0002], [0010], [0020]-[0025], [0027]-[0029], [0033]-[0047]; FIG. 1.



EX1004, FIG. 1 (annotated).

Element [1a]

To start, Salmela discloses that device 10 can be “a cellular communication device, such as a cellular radiotelephone, pager, PDA, computer.” EX1004, [0021]. A POSITA would have recognized that these types of wireless devices all commonly included a ***user interface*** by 2013. EX1003, ¶96 (citing corroborating EX1014, EX1015, 10-15, EX1016, 28-31). Furthermore, Salmela acknowledges that a cellular handset user can “access subscribed services” through a home operator network. EX1004, [0004]. By 2013, accessing such “subscribed services” commonly involved interaction with a ***user interface*** on the wireless device (e.g., voice calls through a speaker and microphone, text messaging through a keypad and/or touchscreen, and internet browsing through a touchscreen). EX1003, ¶96

(citing corroborating EX1014, [0228]-[0300], [0544]-[0575], EX1015, 30, EX1016, 23).

To the extent Salmela does not expressly disclose that its wireless device includes a user interface, it would have been obvious to implement a user interface in Salmela's device based on the teachings of Rishy-Maharaj. EX1003, ¶97-99; *supra*, §V.A.3. Rishy-Maharaj, for example, describes a wireless device 102 that receives user inputs through a user interface of the device 102, e.g., user inputs for selecting subscription plans and managing credentials. *See, e.g.*, EX1005, [0028]-[0046], [0108]-[0121], FIGS. 1A, 1B, 2. Wireless device 102 includes several user interface elements including "device output system 110" and "device input system 112." EX1005, [0058]. Device output system 110 includes "a display system, a speaker system...and the like." EX1005, [0059]. Device input system 112 includes "a keyboard system...a mouse system, a track ball system...and the like." EX1005, [0060]. Other user interface elements of wireless device 102 include "optional user input 120" and "optional display 122." EX1005, [0058], [0066], [0067]. Aspects of the *user interface* of Rishy-Maharaj's wireless device 102 are depicted below in FIG. 1, for example:

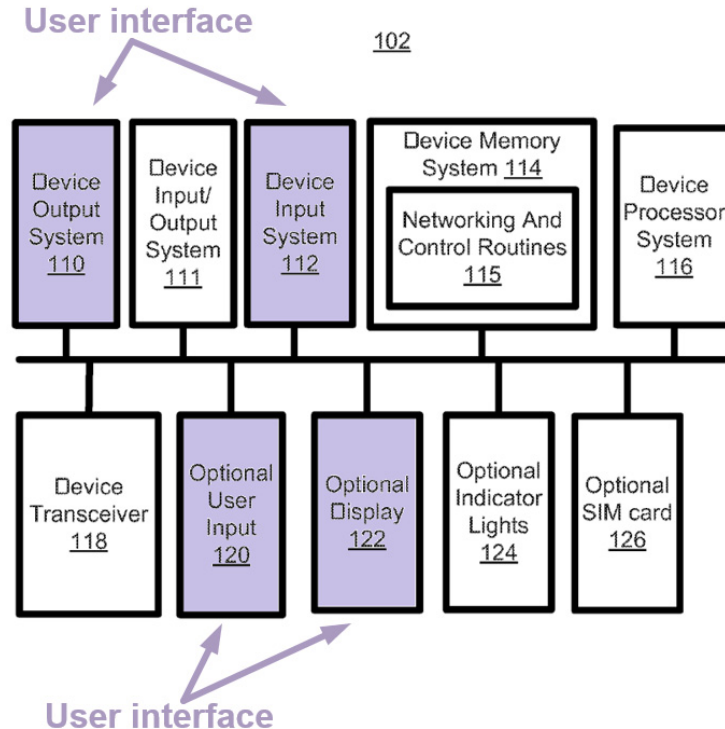


FIG. 1B

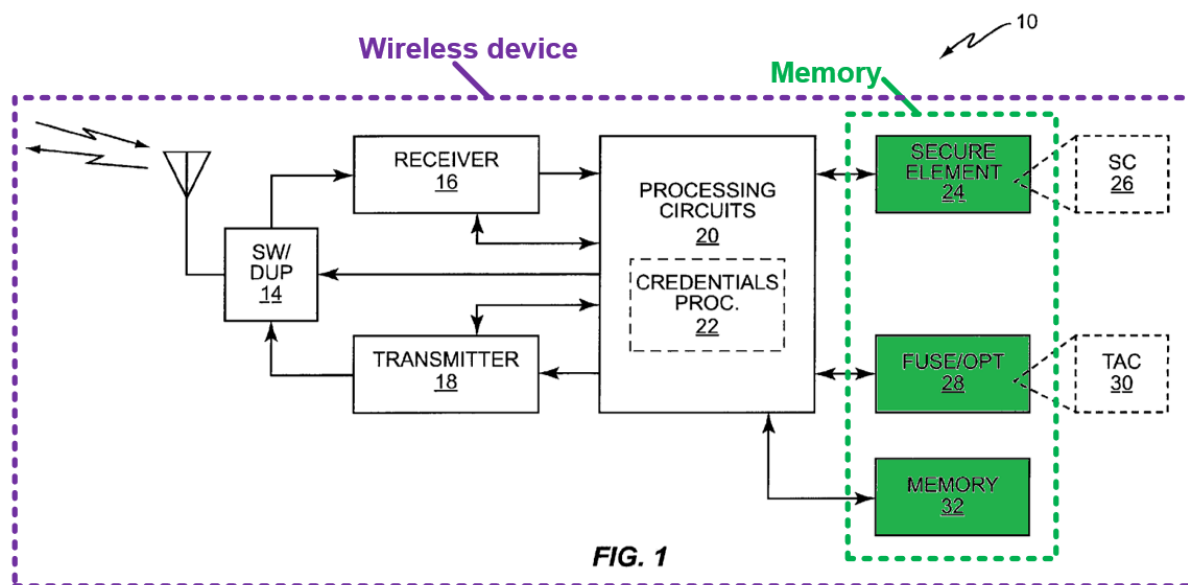
EX1005, FIG. 1B (annotated).

For at least the reasons discussed above (*see* §V.A.3), it would have been obvious and a POSITA would have been motivated to implement Salmela's device 10 to include a user interface as taught in Rishy-Maharaj. EX1003, ¶100. In the Salmela-Rishy-Maharaj combination, a user would beneficially be permitted to perform tasks such as activating or changing a subscription plan through the user interface of the wireless device. EX1003, ¶100.

Element [1b]

Salmela's device 10 has a ***memory*** that includes a secure element 24, a fuse/one-time-programmable (OTP) memory element 28, and a memory 32. EX1004, [0020], [0023], [0025], FIG. 1; EX1003, ¶101-102. Each of these

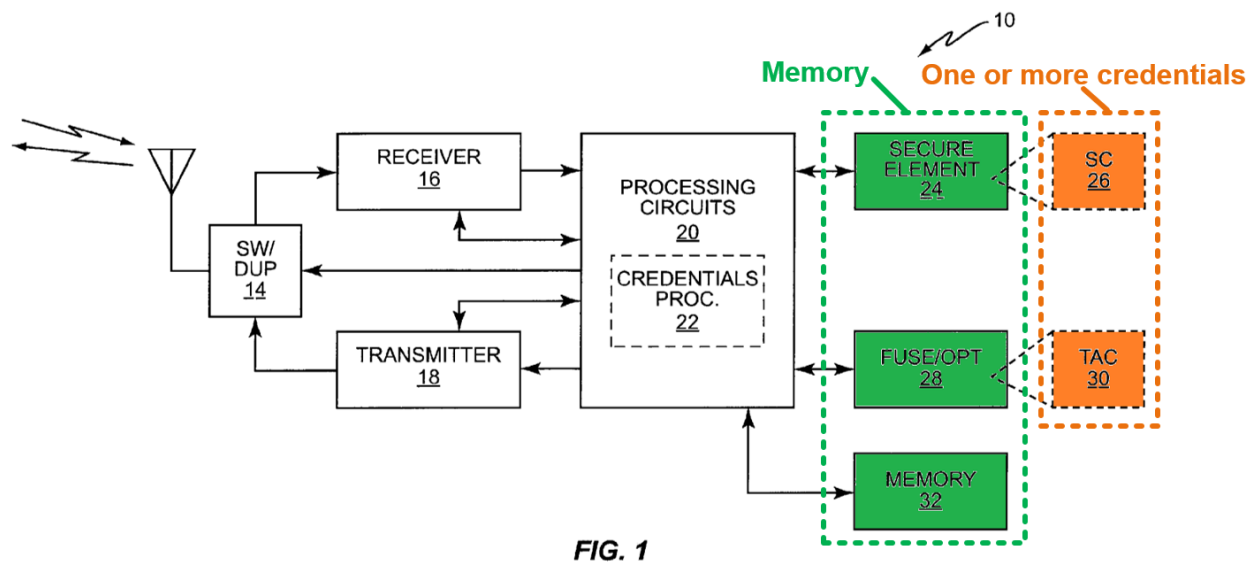
memory components stores information. According to Salmela, secure element 24 can “*store* subscription credentials (SC) 26,” fuse/OTP memory element 28 can “*store* temporary access credentials (TAC) 30,” and memory 32 can “include one or more memory devices, for storing working data, computer program instructions, and configuration information.” EX1004, [0020]. Numerous references corroborate that it was well-known in 2013 for wireless devices to have memory for storing information both persistently and temporarily, including registers, caches, random access memory, secure elements, and the like. EX1003, ¶102 (citing corroborating EX1014, [0095]-[0098], EX1015, 11, 12, 43, 44, EX1016, 146). Aspects of *memory* of Salmela’s device 10 are depicted in FIG. 1, reproduced below. *Cf.* EX1001, 10:14-10:56 & FIG. 2 (explaining that the memory may provide for partitioned or integrated storage of subscription and interim credentials).



EX1004, FIG. 1 (annotated).

Element [1c]

The **memory** of Salmela's **wireless device** (e.g., device 10) is configured to store **one or more credentials associated** with device 10. EX1004, [0010]-[0012], [0020], [0022]-[0025], FIG. 1; EX1003, ¶103-106. For example, secure element 24 stores subscription credentials 26 and fuse/OTP memory element 28 stores temporary access credentials 30. EX1004, [0020], [0022]-[0025], [0027], FIG. 1. These credentials are depicted below in FIG. 1:



EX1004, FIG. 1 (annotated).

Salmela further explains that subscription credentials 26 and temporary access credentials 30 **authorize** Salmela's wireless communication device 10 to use a **wireless access network** to access **one or more services**. EX1004, [0010]-[0012], [0020], [0022]-[0025]; EX1003, ¶104. For instance, Salmela expressly discloses that subscription credentials 26 are “for gaining network access” and that

temporary access credentials 30 are “for gaining temporary access.” EX1004, [0022], *see also* [0012], [0025]. The “network access” described by Salmela provides device 10 access to a **wireless access network** such as a home network and/or a visited network. EX1004, [0010], [0028], [0030]-[0032].

For example, Salmela’s device 10 can use subscription credentials 26 and temporary access credentials 30 to access home network 40 and visited network 46. EX1004, [0028], [0030]-[0032], FIG. 3. Home network 40 includes a radio access network (RAN) 42 and a core network (CN) 44. EX1004, [0028], FIG. 3. Visited network 46 includes RAN 48 and CN 50. EX1004, [0028], FIG. 3. These **wireless access networks** can provide **one or more services** to device 10, such as wireless data service. EX1004, [0004], [0028], [0031]-[0033]; EX1003, ¶¶105-106. Access to the home and visited networks allows device 10 to connect to the internet and access the services of other networks and servers communicably coupled to the home and visited networks. EX1004, [0028]. Temporary access credentials 30 also authorize the device 10 to gain access to a wireless access network to utilize services for obtaining new long-term subscription credentials 26. EX1004, [0028].

Element [1d]

As described above (*see* §V.A.1), Salmela discloses techniques for automatically updating subscription credentials 26 on a device 10. EX1004,

[0003]-[0012], [0020]-[0027]; EX1003, ¶107. Device 10 can determine that new subscription credentials are needed by comparing “first information” corresponding to the subscription credentials 26 currently held by device 10 with “second information” corresponding to subscription credentials “that are considered by [a] registration service to be current for the wireless communication device 10.” EX1004, [0044]; *see also*, [0041]. The first and second information may differ if the user has previously requested to change to a subscription plan requiring new subscription credentials that have not yet been loaded on device 10. EX1004, [0041], [0044].

According to Salmela, the “first information” can be a “hash value” or “time stamp” of the subscription credentials 26 currently held by device 10. EX1004, [0041], [0044]. Likewise, the “second information” can be a “hash value” or “time stamp” of subscription credentials that the registration service considers current for device 10. EX1004, [0041], [0044]. The hash value and/or time stamp of the underlying subscription credential that the registration service considers current each corresponds to and renders obvious a “***target credential***” as recited in element [1d]. EX1003, ¶108.

To this point, Salmela’s hash value and/or time stamp for the subscription credentials considered current by the registration service are analogous and substantially similar to examples of the “requested credential” (e.g., target

credential) as described in the '510 Patent specification.² EX1003, ¶109. For example, the '510 Patent explains that the wireless device can receive a requested credential from an “application server or other network element” and that the requested credential may contain only “a subset of information about all of the one or more credentials that were requested to be changed.” EX1001, 11:1-19.

Salmela's hash value and time stamp are likewise received from a remote server and contain a subset of information about the subscription credentials considered by the registration service to be current for device 10 to which the device owner has requested to change. EX1003, ¶109. The '510 Patent's disclosure at col. 11:32-37 is similarly clear that the requested credential (e.g., target credential) can be related, but distinct from, the underlying updated credential (e.g., IMSI) that the

² The term “target credential” is never used in the specification of the '510 Patent, but the descriptions of the “requested credential” in the specification generally align with the “target credential” in claim 1. FIG. 3, for instance, depicts an operation 1164 that involves comparing the device's current credentials with the requested credentials. EX1001, 11:28-37, FIG. 3. Element [1h] similarly refers to “determin[ing] that the particular credential does not match the target credential.” *Id.*, 20:33-34. Similar uses of “requested credential” and “target credential” occur throughout FIG. 3 and claim 1, respectively. EX1003, ¶109.

device uses to authorize itself on a wireless network. *See* EX1001, 11:32-37

(describing the “requested credential” as a “configuration state indicator” related to a phone number, ISDN, or other credential being updated).

Although claim 1 does not require that the “target credential” and underlying “updated credential” be the same, or even that the “target credential” and “updated credential” be similarly formatted, these features nonetheless would have been obvious in the Salmela-Rishy-Maharaj combination by implementing device 10 to receive the underlying subscription credentials (e.g., IMSI) that the registration service considers current for device 10, thereby allowing for direct comparison at device 10 between those credentials and the subscription credentials 26 currently held by the device (e.g., a direct IMSI comparison), rather than comparing time stamps or hash values.³ EX1003, ¶110. In this case, the underlying subscription credentials that the registration service considers current for device 10 would correspond to and render obvious the claimed “*target credential*.” EX1003, ¶110.

A POSITA would have been motivated to configure device 10 to receive and store the underlying credentials that the registration service considers current for

³ As another predictable option, it would have been obvious for device 10 to compute hash values of both sets of credentials locally for comparison. EX1003, ¶110.

device 10 in their original form in lieu of or in addition to a time stamp and/or hash value to facilitate a straightforward comparison of the credentials in their original form. EX1003, ¶111. This implementation would be beneficial to alleviate the burden on the remote server (e.g., registration server 54) of computing a hash or maintaining a time stamp for the credentials, thereby simplifying aspects of the registration service's operations. EX1003, ¶111. A POSITA also would have considered the choice of performing either a direct comparison of the credentials in their original form or a comparison of values associated with or derived from the credentials (e.g., hash values, time stamps) to be an obvious design choice for which a suitable option would be selected based on the needs and circumstances of a given application or design. EX1003, ¶112. Comparing subscription credentials in their original form or comparing related values such as hashes or time stamps that uniquely represent the underlying subscription credentials would have been understood to equivalently indicate whether device 10 needs to update its current subscription credentials 26. EX1004, [0041], [0044]; EX1003, ¶112. Both options also would have been obvious to a POSITA, especially since Salmela itself already contemplates a range of options for comparing the device's current credentials to a target credential to determine whether new subscription credentials are needed on the device. EX1004, [0043] (“**Broadly**, the wireless communication device 10 ... is

configured to communicate with the registration service to determine whether new subscription credentials are needed.”); *generally*, [0040]-[0045]; EX1003, ¶112.

Salmela also discloses that device 10 receives from the registration server 54 the hash value or time stamp for the credentials that the registration service considers current before comparing that information to the hash value or time stamp of the subscription credentials 26 currently held by device 10. EX1004, [0040], [0041]. A POSITA would have understood this to mean that the memory of device 10 stores the “second information” hash value or time stamp (e.g., target credential) at least temporarily upon receipt as the device 10 prepares to perform the comparison between the “first information” and “second information.” EX1004, [0040]-[0041], [0044] (“second information received from the registration service”); EX1003, ¶113. At the very least, it would have been obvious to store the second information or underlying subscription credentials that the registration service considers current in memory of device 10 for a period of time sufficient for device 10 to perform this comparison. EX1003, ¶113 (citing corroborating EX1027, 40). For example, it would have been obvious for device 10 to store the credentials or “second information” received from the registration server in registers, cache, random access memory, and/or or other memory of device 10 that conventionally make data available to a processor, as would occur for the device to 10 to perform the comparison described at paragraphs [0041] and

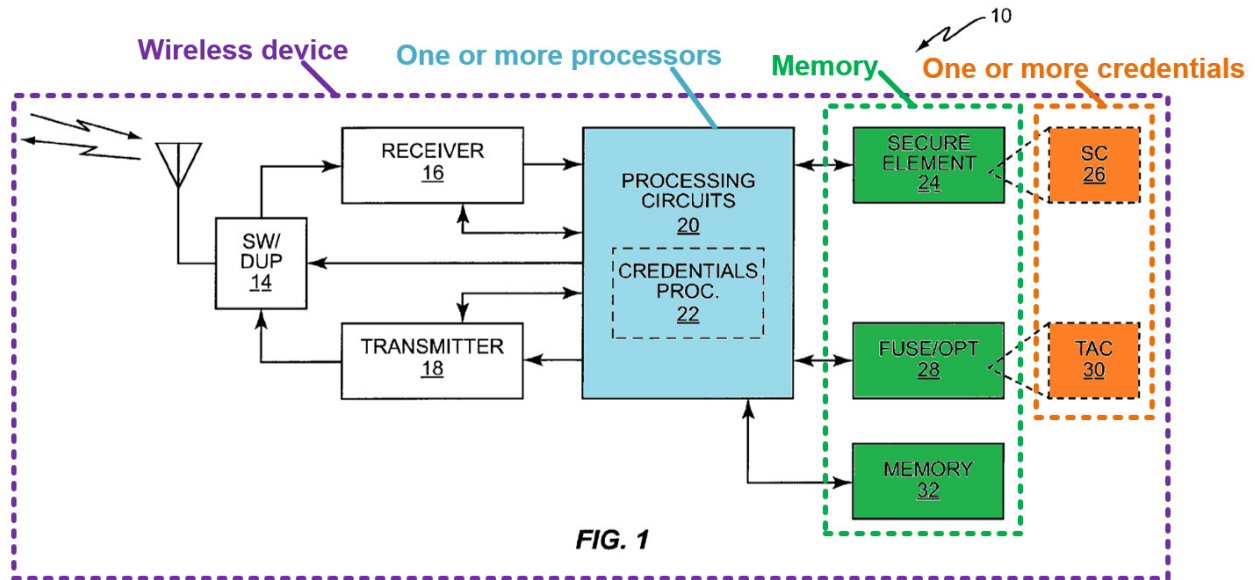
[0044] of Salmela. EX1004, [0041], [0044], [0020] (memory 32 can “include one or more memory devices, for storing working data, computer program instructions, and configuration information”); *supra*, [1b]; EX1003, ¶114.

As another example, it would have been obvious to store the target credential (e.g., hash value, time stamp, or underlying credential) received from the registration service in secure element 24 or a similar memory element to keep such information secure and to ensure it is available for subsequent use, similar to the storage of subscription credentials 26 in secure element 24 as disclosed in Salmela. EX1004, [0020]; EX1003, ¶114.

Additionally, as described further below with respect to [1k], Salmela discloses and renders obvious storing the target credential that the registration service considers current in the secure memory element 24 as an updated credential when device 10 determines that its current subscription credentials 26 are no longer valid. *Infra*, [1k]; EX1003, ¶115.

Element [1e]

Salmela’s device 10 comprises ***one or more processors*** including processing circuits 20 and credentials processor 22. EX1004, [0020], [0024], [0026], [0027], FIG. 1; EX1003, ¶116-117. The ***one or more processors*** are depicted below in FIG. 1:



EX1004, FIG. 1 (annotated).

Salmela discloses that the *one or more processors*—e.g., processing circuits 20 and/or credentials processor 22—*execute one or more machine-executable instructions* that cause the *one or more processors* to perform actions. EX1004, [0020], [0024], [0026], [0027], FIG. 2. For instance, “credentials processor 22 may be implemented via software executing in one or more microprocessor circuits used to implement the processing circuits 20.” EX1004, [0026]. This software represents *machine-executable instructions*. EX1003, ¶117. Furthermore, credentials processor 22 is configured to *execute machine-executable instructions*. See, e.g., EX1004, [0024], [0034]; EX1003, ¶117.

Element [1f]

Salmela describes that a user (referred to as “device owner”) can request to activate or change subscription plans for each of his or her wireless devices

including a device 10. EX1004, [0008] (“the device owner can select and activate subscriptions”), [0009] (“changing subscription plans”), [0011] (“an owner ... can change subscription agreements”), [0053] (“changing subscription information”), Abstract (“new home operator”), [0050] (“device owner can change subscriptions”), [0007]. After the user has submitted a request to change subscriptions, each device associated with the new subscription plan automatically obtains updated subscription credentials associated with the new subscription plan in response to detecting a network-provisioning state change. EX1004, [0003]-[0009], [0011], [0020]-[0027], [0050], FIG. 3; EX1003, ¶118.

The user request to change a subscription plan to a new home operator in Salmela corresponds to and renders obvious “a user request to replace a particular credential of the one or more credentials with the target credential,” as recited in Element [1f]. EX1003, ¶119. By requesting that the device 10 operate under a new subscription plan, the user is requesting that a subscription credential 26 currently held by device 10 (*a particular credential of the one or more credentials*) be replaced with a *target credential* associated with the new subscription plan, and indeed this would have been obvious to a POSITA since the new subscription plan is associated with a new home operator and thus requires new subscription credentials for the device to use a wireless access network to access services

offered by the new home operator under the new subscription plan.⁴ EX1004, [0003], [0010]-[0012]; EX1003, ¶119. For example, Salmela discloses that subscription credentials 26 “generally remain valid for as long as the owner of the device 10 maintains a corresponding subscription agreement with the home network operator that issued the subscription credentials 26.” EX1004, [0022]. Thus, when the user requests to change home operators by canceling a subscription plan, the user is requesting to invalidated the device’s current subscription credentials and replace them with a target credential associated with a new home operator. EX1004, [0007]-[0009], [0022]; EX1003, ¶120.

⁴ As discussed in the analysis of [1d], Salmela’s hash value or time stamp for the subscription credential that the registration service considers current, and the underlying subscription credential that the registration service considers current, each renders obvious and alternatively provides a “*target credential*” in a manner consistent with the ’510 Patent’s description of such features. *Supra*, [1d].

Likewise, Salmela’s current subscription credential 26 on device 10 that would be replaced when the subscription is changed can be indicated by a hash value, time stamp, or the underlying credential 26 itself, each of which maps to and renders obvious a “*particular credential*” as claimed. EX1004, [0041], [0044]; EX1003, ¶119.

To the extent Salmela does not expressly disclose that device 10 obtains an indication of a user request to update a subscription plan *through a user interface* of device 10, this conventional option would have been obvious to a POSITA based on the teachings of Rishy-Maharaj. EX1003, ¶121. As described above in connection with [1a], Rishy-Maharaj discloses a wireless device 102 including a user interface. EX1005, [0028]-[0046], [0058]-[0060], [0066], [0067], [0108]-[0121], FIGS. 1A, 1B, 2. Rishy-Maharaj further discloses that a “user may select [a] subscription plan ... that best suits the user”, and in particular, “[t]he wireless device 102 may [] have an optional user input 120 to allow the user to select a plan.” EX1005, [0112]; *see also*, [0108]-[0121], FIGS. 1B, 2.

As described above in §V.A.3, it would have been obvious for a POSITA to implement Salmela in accordance with Rishy-Maharaj’s teaching such that the user in Salmela would submit a request to change subscription plans through a user interface of his or her device 10. EX1003, ¶122. Doing so would, among other reasons discussed above, enhance the user’s convenience in selecting or changing a subscription plan. EX1003, ¶122; *supra*, §V.A.3. As a result, Salmela’s device 10 in the combination would obtain, through the user interface and based on the user’s selection of a new subscription plan in the user interface, an indication of a user request to replace a particular credential (e.g., subscription credential 26) with the target credential (e.g., a new credential associated with the new subscription plan)

as recited in [1f]. EX1003, ¶123-126; *cf.* EX1001, 12:45-14:40 and FIGS. 4-13

(’510 Patent similarly describing embodiments where the device obtains an “indication” of a user request to replace credentials based on the user’s mere tapping of a “Transfer” button).

Element [1g]

Salmela discloses that device 10 is configured to detect a failure to gain network access using its current subscription credentials 26, and based on such detection, to ***automatically*** revert from current subscription credentials 26 to temporary access credentials 30 as part of an automated process for obtaining new subscription credentials associated with a new subscription plan. EX1004, [0010], [0024], [0025], [0027], [0033]-[0035], FIG. 4. This failure to gain network access indicates that the device 10 is no longer provisioned with valid credentials due to a possible subscription change and represents ***a network-provisioning state change***. EX1003, ¶123-126; *cf.*, EX1001, 9:4:11, 11:20-27 (’510 Patent describing how denied network access events of the same kind disclosed in Salmela indicate network provisioning state changes).

For example, Salmela discloses that device 10 can “detect access loss for its local (preferred) RAN” using subscription credentials 26. EX1004, [0033]. Based on detecting this access loss, device 10 “attempt[s] reconnection using its current subscription credentials 26.” EX1004, [0033]. If reconnection attempts fail, device

10 can “scan for alternative access” and ultimately determine that there has been a failure to gain network access if device 10 is unable to secure alternative access using subscription credentials 26. EX1004, [0034], [0035]. Through these operations, the device 10 detects a “*network-provisioning state change*” indicating that current subscription credentials 26 are no longer usable by the device 10 to gain access to services on the network. EX1003, ¶125.

Salmela’s device 10 also performs actions to *automatically* check the validity of its current subscription credentials and obtain new subscription credentials based on detecting a failure to gain network access, as illustrated below in FIG. 2, for example. EX1004, [0027], *see also* [0033]-[0035], [0037]-[0038], FIG. 4; *infra*, Elements [1h]-[1k]; EX1003, ¶126.

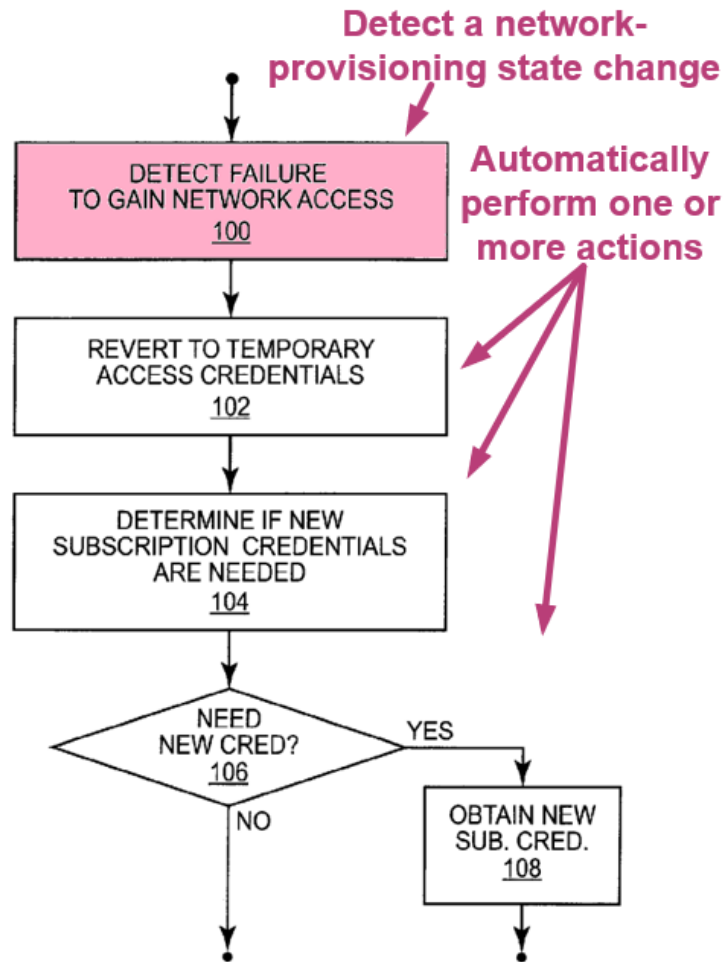


FIG. 2

EX1004, FIG. 2 (annotated).

Element [1h]

Based on detecting a failure to gain network access using its current subscription credentials 26, device 10 automatically reverts to temporary access credentials 30. EX1004, [0010], [0024] (“revert from the subscription credentials 26 to the temporary access credentials 30, responsive to detecting network access failure”), [0027] (“in response to detecting such failure, [] reverting from the current subscription credentials 26 to the temporary access credentials 30”), FIG.

2. Using temporary access credentials 30, device 10 obtains temporary network access and connects with a registration server to determine whether new subscription credentials are available for device 10. EX1004, [0010], [0027] (“determining whether new subscription credentials are needed based on gaining temporary network access via the temporary access credentials”), FIG. 2; EX1003, ¶127-129.

As described above in connection with Elements [1d] and [1f], Salmela’s device 10 automatically identifies a need for new subscription credentials by determining that its current subscription credential 26 (*particular credential*) does not match the subscription credential that the registration service considers to be current (*target credential*). EX1004, [0041], [0044]; *supra*, Elements [1d], [1f]. Salmela describes options for determining this mismatch by comparing either hash values or time stamps respectively associated with the device’s current subscription credential 26 and the credential that the registration service considers current, although it would have been equally obvious to directly compare the underlying credentials themselves.⁵ EX1004, [0020]-[0027], [0041], [0044]; EX1003, ¶130-132.

⁵ Recall that Salmela’s hash values, time stamps, and underlying credentials (e.g. IMSI) all provide alternative forms of the claimed “*particular credential*” and

A process for automatically determining that new credentials based on detecting a *network-provisioning state change* is depicted below in FIG. 2 of Salmela:

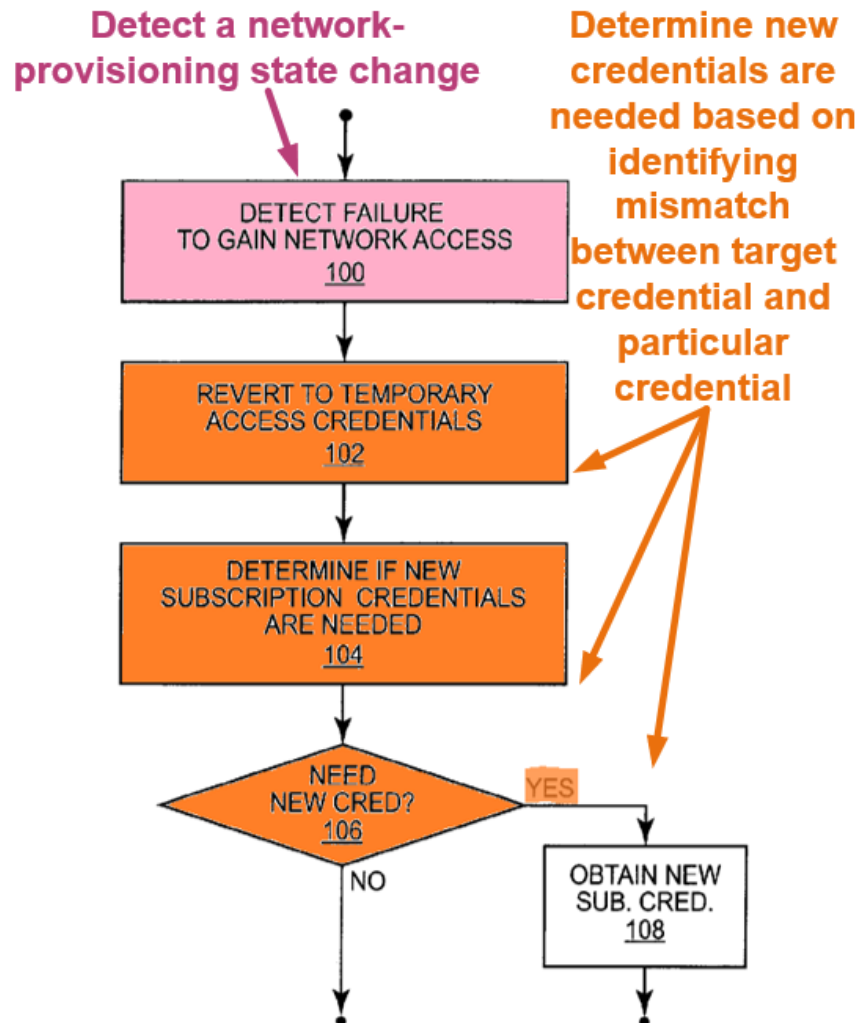


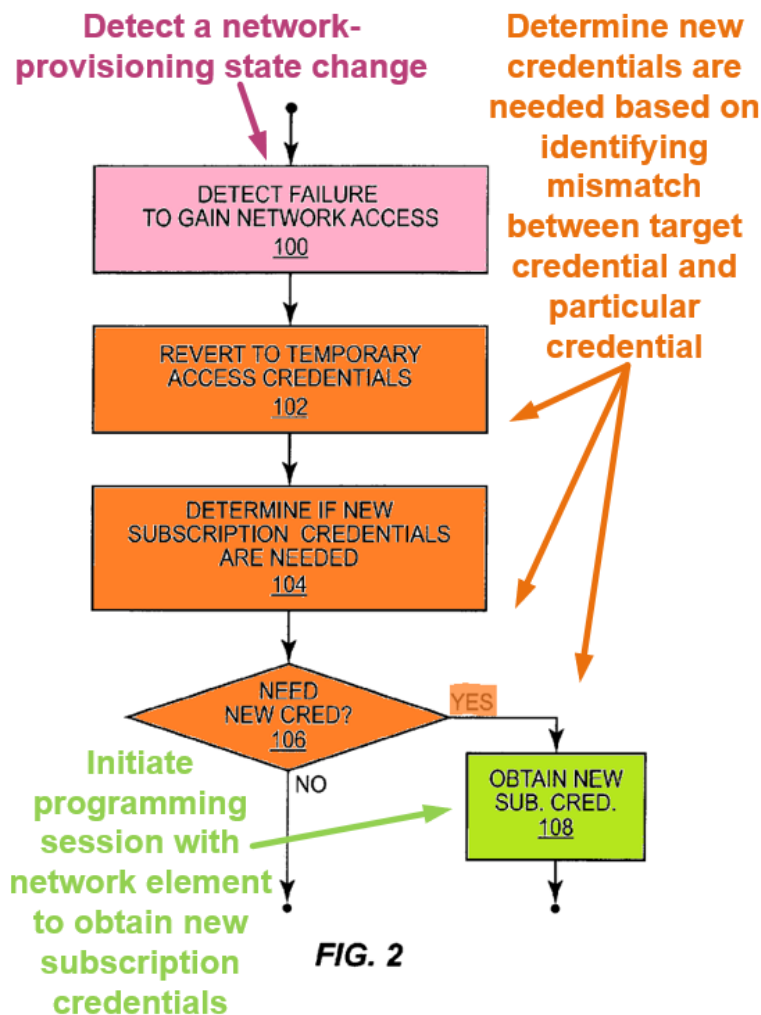
FIG. 2

EX1004, FIG. 2 (annotated).

“*target credential*” consistent with disclosures in the ’510 Patent itself. *Supra*, [1d], [1f]; EX1003, ¶130.

Element [1i]

Salmela discloses that device 10 can *initiate a programming session* with a *network element* to obtain new subscription credentials. EX1004, [0025]-[0027]; EX1003, ¶133-137. An example process for automatically initiating a programming session to obtain new subscription credentials is depicted below in FIG. 2:



EX1004, FIG. 2 (annotated).

To obtain the new subscription credentials, Salmela's device 10 receives "network address information from the registration service that identifies a credentialing server from which the new subscription credentials are to be obtained." EX1004, [0045]; EX1003, ¶134. Using this network address information, device 10 initiates a programming session with a "credentialing server"—a *network element*—to obtain the new subscription credentials. EX1004, [0045], *see also* [0025]. Device 10 *automatically* performs these operations based on its detection of a network access failure (*network-provisioning state change*). EX1004, [0011], [0025], claim 25; EX1003, ¶135.

Salmela's *network element*—e.g., the "credentialing server"—is communicatively coupled to device 10 over the wireless access network. EX1003, ¶136. For example, Salmela discloses that "the credentialing server is, in one or more embodiments, an entity in...the CN of the service provider that issued the new subscription credentials." EX1004, [0045]. In the telecommunications field, "CN" refers to "core network," which is an aspect of a wireless access network and which can be accessed through the radio access network ("RAN") of the wireless access network. EX1004, [0028], FIG. 3; EX1003, ¶136 (citing corroborating EX1017, 6, EX1018, 2).

The credentialing server is located in the core network of the wireless access network that issues subscription credentials for the device 10 to access one or more

services. EX1004, [0028], FIG. 3. Device 10 is accordingly communicatively coupled to the credentialing server over the wireless access network. EX1003, ¶137.

Element [1j]

Through the *programming session* initiated with the *network element* (“credentialing server”), device 10 can obtain an *updated credential* (e.g., a new subscription credential) from the credentialing server.⁶ EX1004, [0025], [0027], [0045] (“contact the credentialing server to obtain the new subscription credentials”), FIGS. 2, 4. The updated subscription credentials obtained from the credentialing server and associated with the new subscription plan replaces the subscription credentials 26 on device 10 associated with the prior subscription

⁶ Like Salmela, the ’510 Patent explains that the updated credential can be the target credential or the target credential can be a representation of the updated credential. EX1001, 9:16-19 (“mobile device 100 detects that a current device credential does not match the expected credential”), 9:47-49 (“delivers the new device credentials to the device”), 10:42-44 (“stores the expected credentials to be programmed to mobile device 100”); EX1003, ¶138.

plan.⁷ EX1003, ¶138. Device 10 obtains the updated subscription credentials *automatically* through the process that occurs based on the device’s detection of a network access failure (*network-provisioning state change*). EX1004, [0011], [0025], [0048], claim 25; EX1003, ¶138.

Element [1k]

Salmela teaches, for example, that device 10 “uses its temporary access to obtain new subscription credentials, which it may download to its secure element 24.” EX1004, [0025], *see also* [0036] (“newly obtained subscription credentials become the device’s current subscription credentials 26”), [0046]. As described above in connection with Element [1b], *supra*, the memory of device 10 includes secure element 24. EX1004, [0020], [0025]. Device 10’s processors thus assist in storing the updated credential (e.g., the “new subscription credential”) in the

⁷ In at least two instances, Salmela uses both of the terms “new” and “updated” to refer to subscription credentials obtained using temporary access credentials. EX1004, [0011] (“new/updated subscription credentials”), [0036] (“[t]he device 10 then uses that temporary network access to obtain new subscription credentials (Block 126), which comprises downloading a new or updated USIM”). Salmela further teaches that “[o]nce the device 10 obtains new subscription credentials, they replace its previously current subscription credentials.” EX1004, [0036].

memory. EX1003, ¶139. The updated credentials replace the prior subscription credentials *automatically* based on the device's detection of a network access failure (*network-provisioning state change*). EX1004, [0011], [0048], [0025], claim 25; EX1003, ¶139.

Claim [2]

Salmela discloses that its process of checking for and updating subscription credentials is a recurring process that occurs whenever current subscription credentials are unable to provide network access. EX1004, [0010], [0020]-[0027], FIGS. 1-2; *supra*, Elements [1g]-[1k]; EX1003, ¶140-144. This process can result in current subscription credentials 26 being replaced with new/updated subscription credentials. EX1004, [0025], [0027]. The new/updated subscription credentials then become the current subscription credentials, replacing the previous credentials that failed to gain network access. EX1004, [0036], [0046]; *supra*, Element [1k]. After device 10 replaces a *particular credential* (e.g., current subscription credentials 26) with an *updated credential* (e.g., new subscription credentials) as described in Elements [1f]-[1k], *supra*, device 10 uses the same automatic process to replace the *updated credential* (e.g., new subscription credentials) when Salmela's device 10 detects that the new subscription credentials fail to gain network access. EX1004, [0046] ("in case further reversions are needed"); EX1003, ¶140.

After the ***updated credential*** (e.g., new subscription credentials) replaces the ***particular credential*** (e.g., the previously current credential) based on device 10 detecting a network access failure using the ***updated credential***, device 10 can perform another comparison—this time between a hash value corresponding to the ***target credential*** (which the registration service considers to be current for device 10) and a hash value corresponding to the ***updated credential*** (which is now the current subscription credential 26). EX1004, [0020]-[0027], [0041], [0044] [0049]-[0056], FIGS. 1-2; *supra*, Elements [1g]-[1k]; EX1003, ¶140-142. A POSITA would have understood and it would have been obvious that a mismatch would be determined between the hashes for the ***updated credential*** and ***target credential*** if the value of the ***target credential*** changes for any reason after the device begins using its ***updated credential*** as the current subscription credential. EX1003, ¶142. The mismatch can also be determined based on comparison of time stamps or the underlying credentials, as described above. *Supra*, Elements [1d], [1k].

Salmela teaches that the value of the ***target credential*** can change, for example, when the user makes another request to change the home operator or subscription plan thereby causing the registration service to update the ***target***

credential according to the request.⁸ EX1004, [0010]-[0012], [0050], FIGS. 2, 4.

Even if the user has not requested to activate a new subscription plan or to change the home operator and the **target credential** has not changed at the registration service, it would have been obvious that the device 10 would still detect a mismatch between the hashes for the **updated credential** and **target credential** if the hashes or the credentials themselves have been corrupted at device 10 (e.g., as a result of transmission or memory errors). EX1003, ¶143 (citing corroborating EX1019, 4).

Based on determining that the updated credential does not match the target credential, device 10 can take an **action**, e.g., “identify[ing] a credentialing server from which [] new subscription credentials are to be obtained, and using the temporary network access to obtain the new subscription credentials.” EX1004, [0045]; *see also*, [0026], [0027]; *infra*, Claims [3], [6]; EX1003, ¶144.

Claim [7]

⁸ The '510 Patent confirms that the target credential—sometimes referred to as the “requested credential” or “expected credential”—is not necessarily static. The value of the target credential can change whenever a new phone number or other credential is submitted as the target of a phone number or other credential porting process. EX1001, 9:11-27, 10:42-51, 7:1-15, FIG. 2; EX1003, ¶143.

Salmela's ***updated credential*** (e.g., new subscription credentials) can replace the formerly current subscription credentials 26 representing the ***particular credential*** to become the current subscription credentials stored in secure element 24. EX1004, [0020]-[0027], [0036], [0040], [0041], [0044]-[0047]; *supra*, Elements [1g]-[1k]; EX1003, ¶148-151. When device 10 replaces current subscription credentials 26 with new subscription credentials, device 10 retains temporary access credentials 30 "in case further reversions are needed." EX1004, [0046]. Indeed, Salmela discloses that another reversion to temporary access credentials 30 is needed when the ***updated credential*** represented by the new subscription credentials fails to gain network access. EX1004, [0047]. Salmela's device 10 can determine whether a new subscription credential is needed based on comparing a hash value or other information about the ***updated credential*** (e.g., the new current subscription credential 26) with a hash value or other information about the ***target credential*** (e.g., subscription credentials considered by the registration service to be "current" for device 10). EX1004, [0041], [0044].

When device 10 determines that the ***updated credential*** matches the ***target credential*** based on comparing the hash values, device 10 ***takes an action*** to return to using the ***updated credential***. EX1004, [0047] ("returns to using its current subscription credentials 26"). In this context, a POSITA would have understood and it would have been obvious that a match would be determined between the

updated credential and the *target credential*, for example, when the user has not requested to activate a new subscription or to change home operators and the target credential held by the registration service has not changed since the device 10 began using the *updated credential*. EX1004, [0040]-[0044], [0053]; EX1003, ¶151.

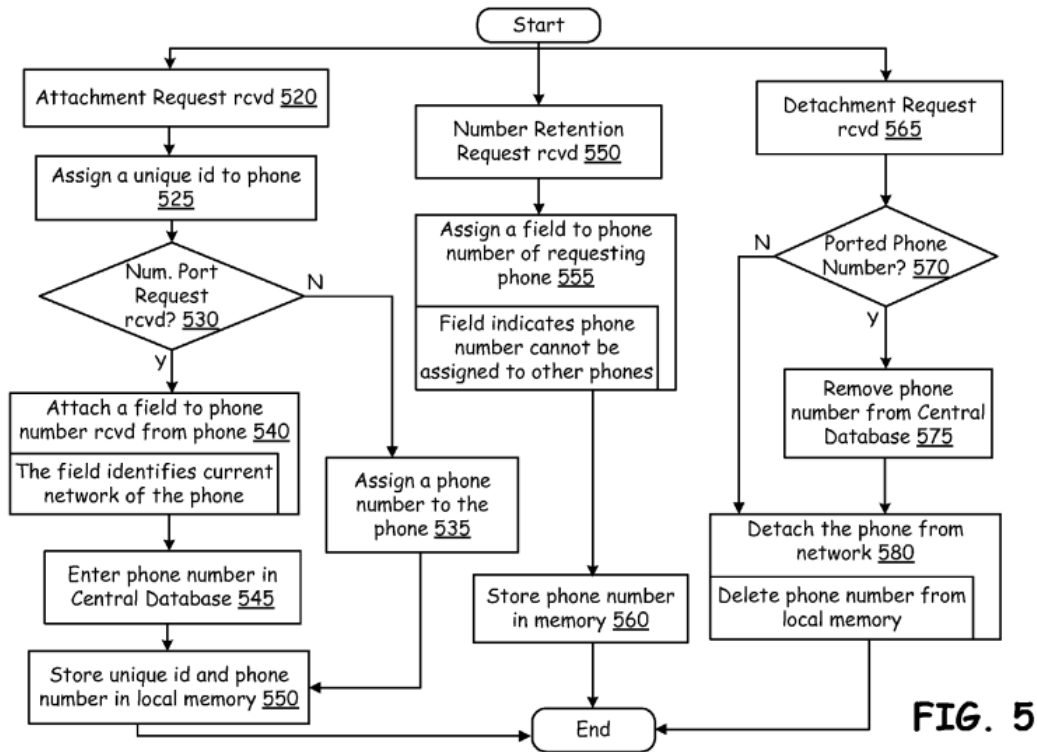
Claim [38]

Salmela expressly discloses that device 10 uses a *temporary credential* (e.g., a temporary access credential 30) to contact the *network element* (e.g., the credentialing server). EX1004, [0025] (“device 10...uses those temporary access credentials 30 to gain temporary network access”), [0045] (“using the temporary network access to contact the credentialing server to obtain the new subscription credentials”). EX1003, ¶191.

B. GROUND 1B: Salmela, in view of Rishy-Maharaj, and further in view of Bennett would have rendered obvious claims 21, 23, and 25

1. Bennett

Bennett describes techniques that allow a wireless phone to retain a phone number or obtain a new phone number at which the phone can be dialed when switching from a current service provider network to a new service provider network. EX1006, [0008], [0009], [0021], [0023]-[0028], [0042]-[0045], FIGS. 1, 5; EX1003, ¶44.



EX1006, FIG. 5.

2. The Salmela-Rishy-Maharaj-Bennett Combination

As described above in Ground 1A, Salmela discloses techniques for automatically updating subscription credentials for a wireless device when the device fails to gain network access using its current subscription credentials and a user has requested to change subscription plans or the home operator network for the device. *Supra*, §V.A.1. Salmela explains that the subscription credentials are credentials that allow the wireless device to authenticate itself on a wireless network such as an international mobile subscription identity (IMSI). EX1004, [0012], [0023]. Salmela does not limit the application of its techniques to just IMSI-based embodiments, but instead recognizes that its “methods and apparatuses

may be implemented in a variety of system and device types.” EX1004, [0057]. To the extent Salmela does not expressly identify other suitable subscription credentials, however, a POSITA would have known of other such credentials—such as a non-IMSI phone number used to route calls to a phone—as evidenced by Bennett. *Supra*, §V.B.1; EX1003, ¶45-47. For example, Bennett describes techniques that “allow[] a phone to retain its number while switching from a current network to another network,” where the phone number is specifically “one that is dialed by a calling party” to reach the phone.⁹ EX1006, [0021].

Multiple reasons would have led a POSITA to implement Salmela’s subscription credentials to include a dialable phone number in accordance with Bennett’s suggestion (e.g., MSISDN or MDN). EX1003, ¶47. For example, the ability to update the dialable phone number of Salmela’s device 10 would have beneficially allowed the device 10 to be reached at a new phone number under a new subscription plan—including a phone number that the user ported from

⁹ A POSITA would have understood the phone numbers described in Bennett to be phone numbers that can be dialed to reach the device associated with those numbers. For example, the phone numbers described in Bennett may be a mobile station international subscriber directory number (MSISDN) in a GSM network or a mobile directory number (MDN) in a CDMA network. EX1003, ¶46.

another device. Wireless phones were also conventionally assigned dialable phone numbers in addition to an IMSI before the Critical Date. Even the '510 Patent's own description of background technology recognized that a "phone number" was a known credential for authenticating a mobile device in a wireless network.

EX1001, 5:21-45. A POSITA would have reasonably expected success implementing the combination given the common use of dialable phone numbers by the Critical Date of the '510 Patent. EX1003, ¶47.

3. *Application to Challenged Claims*

Claim [21]

To the extent Salmela does not disclose that the ***one or more credentials*** stored by device 10 include a dialable ***phone number*** which can be called to reach the device 10, Bennett provides this feature. EX1003, ¶213. Bennett discloses that a wireless device (e.g., cellular phone) is configured to store a dialable ***phone number***. EX1006, [0008], [0009], [0021]-[0023]. In the predictable Salmela-Rishy-Maharaj-Bennett combination, Salmela's device 10 would store ***one or more credentials*** including a dialable ***phone number***. *Supra*, §V.B.2.

Claim [23]

To the extent Salmela does not disclose that the ***target credential*** stored by device 10 includes a dialable ***phone number***, Bennett provides this feature. *Supra*, §§V.B.1-2; EX1003, ¶214-215. For example, Bennett discloses the predictable option of switching dialable phone numbers on wireless devices. EX1006, [0025]-

[0028], [0042]-[0045] FIG. 1, FIG. 5. Because the *target credential* of Salmela's device 10 is of the same type as current subscription credentials 26 to enable comparison of the credentials, it would have been obvious that the *target credential* in the Salemla-Rishy-Maharaj-Bennett combination would include a dialable *phone number* (e.g., a new phone number associated with a new subscription). EX1006, [0025]-[0028], [0042]-[0045] FIG. 1, FIG. 5; *supra*, §V.B.2.

Claim [25]

Bennett explains that when a wireless device switches home operators, the device can “receive a new phone number from the new network.” EX1006, [0023], *see also* [0009], [0030]. In the predictable Salmela-Rishy-Maharaj-Bennett combination, the *target credential* that is considered “to be current” would therefore represent a *second* dialable *phone number* different from the *first* dialable *phone number* of current subscription credentials 26 in cases where the device 10 is assigned a new phone number in response to a user requested home operator change. EX1006, [0009], [0023]; EX1004, [0010]-[0012], [0041], [0044]; *supra*, Claims [21], [23]; *supra*, §V.B.2; EX1003, ¶216.

C. GROUND 1C: Salmela, in view of Rishy-Maharaj, further in view of Bennett, and further in view of FCCReg would have rendered obvious claims 26 and 27

1. *FCCReg*

FCCReg is a Federal Register publication dated June 22, 2010 setting forth final agency rules from the Federal Communications Commission (FCC) regarding “Local Number Portability Porting Interval and Validation Requirements” and “Telephone Number Portability.” *See* EX1012; EX1003, ¶48. FCCReg explains that the FCC “adopted standardized data fields for simple number porting to streamline the port process and enable service providers to accomplish simple *wireline-to-wireline* and *intermodal* ports.” EX1012, 1. The term “intermodal ports” refers to “the porting of numbers from wireline providers to wireless providers, and vice versa.” EX1012, 1. Thus, FCCReg details requirements for porting phone numbers between wireline devices (wireline-to-wireline ports) and porting phone numbers between landlines and wireless devices (wireline-to-wireless ports and wireless-to-wireline ports). EX1012, 1, 11; EX1003, ¶48.

For example, FCCReg provides that “[a]ll telecommunications carriers required by the commission to port telephone numbers must complete a simple wireline-to-wireline or simple intermodal port request within one business day,” and acknowledges that the FCC has “established obligations for...porting between wireless providers.” EX1012, 1, 11; ; EX1003, ¶49. Thus, FCCReg demonstrates

that at least as early as June 2010, telecommunications carriers were required by law in the United States to port a number between wireless devices (e.g., from a first wireless device associated with a first wireless carrier to a second wireless device associated with a second wireless carrier). EX1012, 11. Additionally, telecommunications carriers were required to port a number from a landline to a wireless device (e.g., from a wireline carrier to a wireless carrier). EX1012, 1, 11.

2. *The Salmela-Rishy-Maharaj-Bennett-FCCReg Combination*

To the extent Salmela, Rishy-Maharaj, and Bennett do not expressly disclose a wireless phone that obtains a new phone number from another wireless device or from a land line, these features would have been obvious when further considering the teachings of FCCReg. EX1012, 1, 11 (explaining that the FCC has regulated porting “between wireless providers” and porting “from wireline providers to wireless providers”), 6, 11. Multiple reasons would have led a POSITA to implement the device 10 of the Salmela-Rishy-Maharaj-Bennett combination with landline-to-wireless and wireless-to-wireless number porting in accordance with FCCReg’s suggestion. EX1003, ¶50-53.

For example, a POSITA would have sought to implement the device 10 of the Salmela-Rishy-Maharaj-Bennett combination further in accordance with FCCReg’s suggestion to support porting numbers from landlines and other wireless devices because doing so would allow a user to maintain a number from

an older mobile phone or landline on a new mobile phone. EX1003, ¶51. In addition, a POSITA would have been motivated to implement the device 10 of the Salmela-Rishy-Maharaj-Bennett combination with FCCReg's suggestion to permit porting of previously-used phone numbers because the available phone numbers are limited. EX1003, ¶52. Furthermore, implementing device 10 of the Salmela-Rishy-Maharaj-Bennett combination with FCCReg's suggestion to enable number porting from other wireless devices and landlines would have been obvious as a predictable application of a known technique (e.g., enabling number porting) to a known system to achieve merely predictable results. *KSR*, 550 U.S. at 417. A POSITA would have reasonably expected success implementing the combination given the common use of dialable phone numbers by the Critical Date of the '510 Patent. EX1003, ¶53.

3. *Application to Challenged Claims*

Claim [26]

FCCReg describes a federal regulation that requires service providers to permit a ***first wireless device*** to update its phone number from a ***first phone number*** to a ***second phone number***, the ***second phone number*** being previously associated with a ***second wireless device***. EX1012, 1-11; EX1003, ¶217-219. For example, FCCReg requires all service providers to support local number portability (LNP) to allow "porting...between wireless providers." EX1012, 1, 6. This

regulation covers cases where a user replaces his current wireless phone (*second wireless device*) associated with a current phone number (*second phone number*) with a “new” wireless phone (*first wireless device*) that was previously used by somebody else under another phone number (*first phone number*), the user seeking to replace the *first phone number* with the *second phone number* to maintain his current contact. EX1012, 1, 6; EX1003, ¶217-218.

Because porting a phone number between wireless service providers was both well-known and *obligated* by 2010 as taught by FCCReg, it would have been obvious long before the Critical Date for wireless service providers to support a customer in porting a phone number from an old wireless device on an old service provider network to a new wireless device on a new service provider network. EX1012, 1; EX1003, ¶217-219. Consequently, implementing device 10 of the Salmela-Rishy-Maharaj-Bennett combination with FCCReg’s requirement to enable porting between wireless service providers would result in device 10 updating from a *first phone number* to a *second phone number* that was previously associated with a *second wireless device* associated with another service provider. EX1012, 1, 6, 11; EX1003, ¶219.

Claim [27]

FCCReg describes a federal regulation requiring service providers to permit a *first wireless device* to update its phone number from a *first phone number* to a

second phone number, the *second phone number* being previously associated with a *land line*. EX1012, 1, 11. For example, FCCReg discloses that “[a]ll telecommunications carriers...must complete a...simple intermodal port request within one business day.” EX1012, 11. These “intermodal ports” include “wireline-to-wireless ports” in which a phone number is ported from a *land line* to a *wireless device*. Consequently, implementing the device 10 of the Salmela-Rishy-Maharaj-Bennett combination with the requirements of FCCReg would result in the device 10 updating from a *first phone number* to a *second phone number*, the *second phone number* being previously associated with a *land line*. EX1012, 11; EX1003, ¶220.

D. GROUND 1D: Salmela, in view of Rishy-Maharaj, and further in view of Ionescu would have rendered obvious claims 12, 13

1. *Ionescu*

Ionescu describes a wireless device that attempts to establish an emergency communication session by placing a voice call or sending a text message, identifying a network access failure by determining that the emergency communication session was not established, and performing actions based on identifying the network access failure. EX1007, [0011]-[0013], [0018], [0034]-[0042], Cl. 7, FIG. 4; EX1003, ¶54-56.

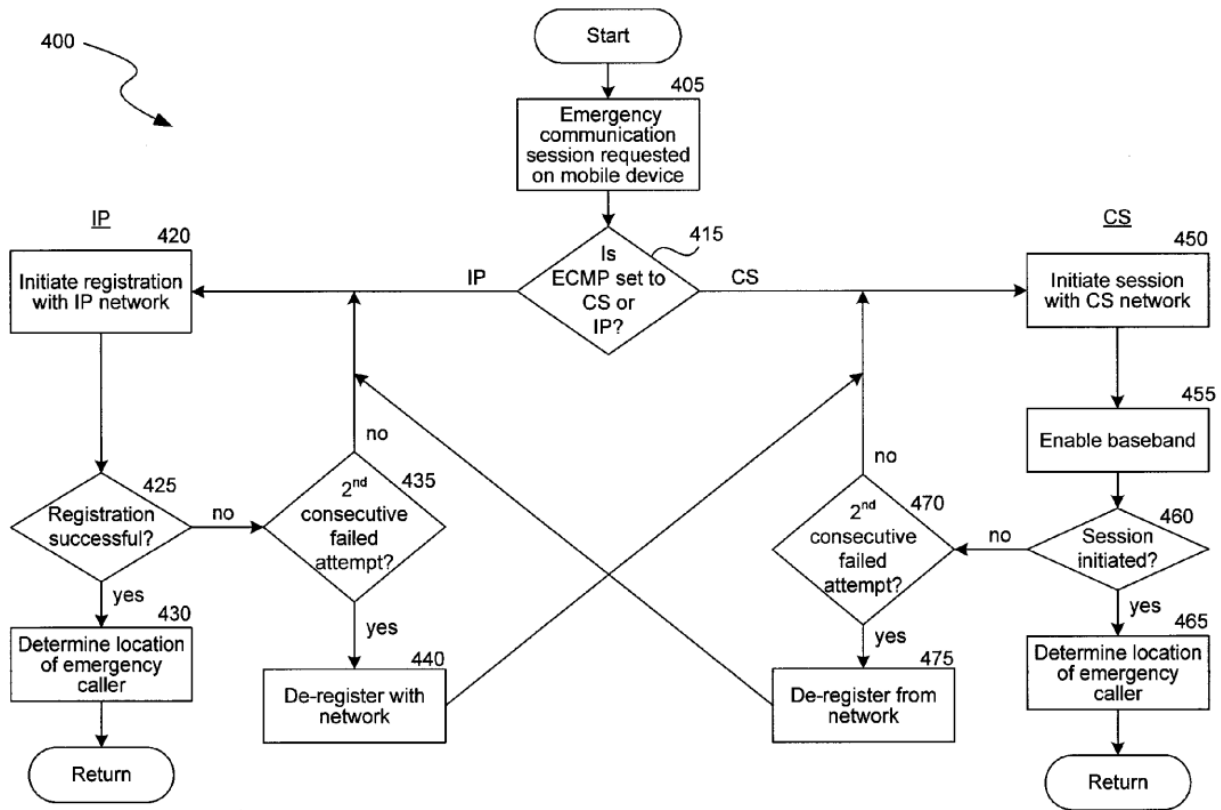


Fig. 4

EX1007, FIG. 4.

2. *The Salmela-Rishy-Maharaj-Ionescu Combination*

Salmela discloses that device 10 can detect a failure to gain network access using current subscription credentials 26, and in response, initiate a process to update the current subscription credentials 26. EX1004, [0020]-[0027], FIGS. 1-2. To the extent Salmela does not expressly disclose examples where device 10 detects the failure to gain network access based on a failed attempt to place a voice call or a failure to send a text message, these features nonetheless would have been obvious in view of Ionescu. Multiple reasons would have prompted a POSITA to

implement Salmela's device 10 in accordance with Ionescu's suggestions for detecting a failure to place a voice call or send a text message before the alleged invention of the '510 Patent. EX1003, ¶57-62.

For example, a POSITA would have understood that implementing Salmela's device 10 to detect a network access failure by detecting a failure to place a call or send a text would predictably provide a way for device 10 to detect network access failure based on communication modes (e.g., calls and text messages) that device 10 commonly uses the network to achieve. EX1003, ¶58. Furthermore, in examples where a user requests to change wireless access networks, a POSITA would have been prompted to use Salmela's process to automatically update subscription credentials 26 in response to detecting a failure to place a phone call or send a text message because these network changes often result in situations where current subscription credentials are insufficient to place calls or send text messages over the new network. EX1003, ¶59. Implementing Salmela's device 10 to detect network access failure based on failed voice calls and texts would have also been obvious to a POSITA because a common feature of cellular communication devices such as Salmela's device 10 is an ability to make emergency communications such as the calls and texts described in Ionescu. EX1003, ¶60.

Implementing Salmela's device 10 to detect network access failure based on failed voice calls and texts as suggested by Ionescu would have been obvious as a predictable application of a known technique to a known system as taught by Salmela to achieve merely predictable results. *KSR*, 550 U.S. at 417; EX1003, ¶61. Furthermore, because there are a finite number of ways to detect network access failure—two prominent examples being failed calls and failed texts—it would have been obvious to try implementing device 10 with Ionescu's suggested techniques for detecting failed calls and failed texts. *KSR*, 550 U.S. at 417; EX1003, ¶61.

Considering the predictable electrical/network and software components involved in the combination and the relatively advanced state of the art at the time, a POSITA would have reasonably expected success applying Ionescu's teachings for detecting a failure to gain network access based on failed voice calls or texts to Salmela before the Critical Date. EX1003, ¶62. Salmela itself invites the use of "multiple methods of detecting a failure to gain network access" and acknowledges that its techniques are not limited by the specific examples disclosed therein. EX1004, [0033], [0057]-[0058]. Ionescu's proposal to detect network access failures based on failed voice calls and texts is thus consistent with the multiple detection methods contemplated in Salmela. EX1003, ¶62.

3. *Application to Challenged Claims*

Claims [12], [13]

Ionescu discloses techniques for determining that an attempt by a wireless device to place a ***voice call*** or send a ***text message*** to establish a voice-based communication session has ***failed***. EX1007, [0029], [0035] (“[A] user of a mobile device initiates an emergency communication session. The emergency communication session may be a voice call (e.g., a 911 call), a text message, or any other emergency request”), [0036]-[0037] (“two consecutive failures to access the network ...”), Cl. 7, FIG. 4; *supra*, §V.D.1. For the reasons described above in §V.D.2, *supra*, it would have been obvious to implement Salmela’s technique for detecting a failure to gain network access with the device 10 by determining that an attempt by the device 10 to place a ***voice call*** or send a ***text message*** has failed as taught in Ionescu. EX1003, ¶221 (including claim [12] and claim [13] analysis).

E. GROUND 1E: Salmela, in view of Rishy-Maharaj, and further in view of Sigmund would have rendered obvious claims 4, 5, 8-10

1. *Sigmund*

Sigmund describes a mobile device 118 that displays notifications to a user about the state of the device and a voicemail password reset procedure. EX1008, [0003]-[0008], [0028]-[0040], FIGS. 1-3; EX1003, ¶63-64.

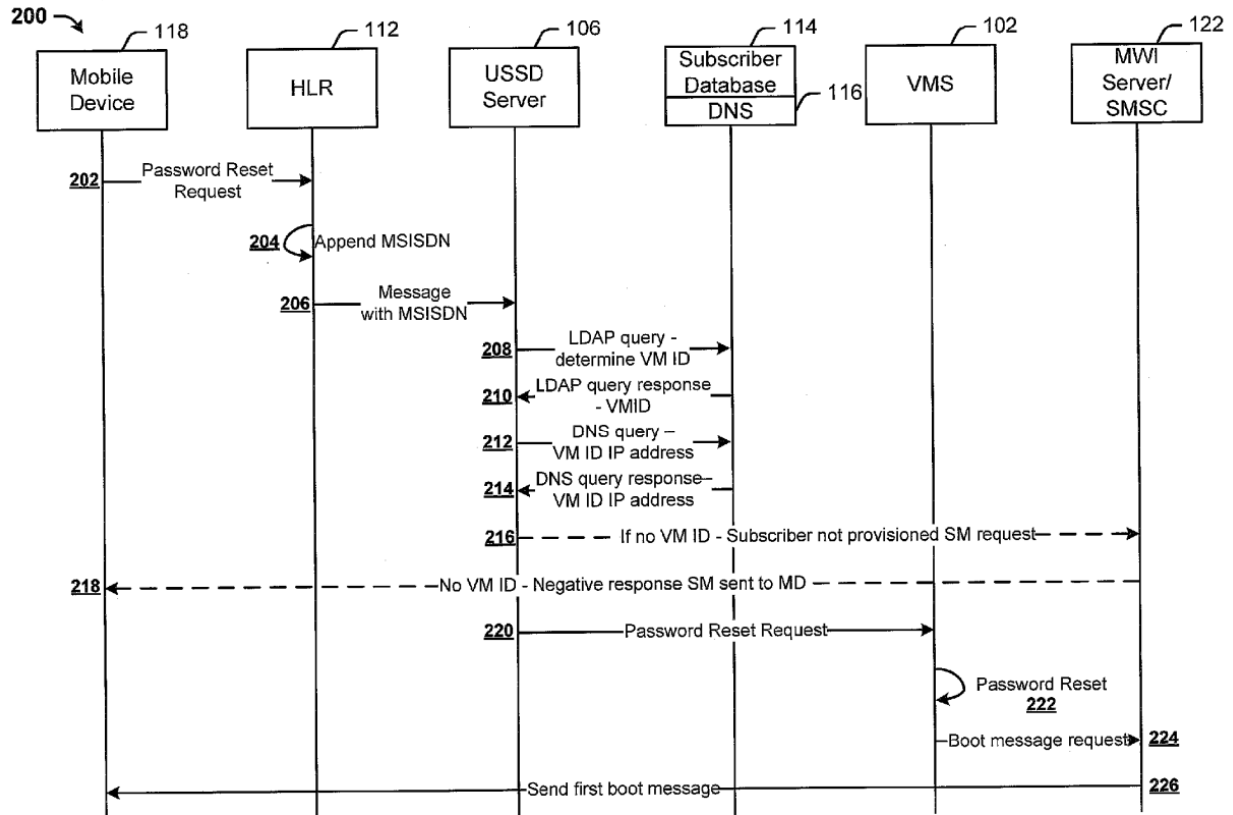


FIG. 2

EX1008, FIG. 2

2. *The Salmela-Rishy-Maharaj-Sigmund Combination*

To the extent that the Salmela-Rishy Maharaj combination does not expressly describe notifications that would be displayed on a user interface of the device in connection with Salmela's credential updating process, these features would have been obvious based on Sigmund. EX1003, ¶65. Multiple reasons would have prompted a POSITA to implement Salmela's device 10 in accordance with Sigmund's suggestion for causing notifications to be sent and displayed on a wireless device before the alleged invention of the '510 Patent. EX1003, ¶66.

For example, a POSITA would have understood that causing notifications to be presented through a user interface of device 10 in connection with Salmela's credential updating process would increase user satisfaction for many users by informing the user of the status of the credential update and notifying the user of particular milestones or events in the process. EX1003, ¶67. Additionally, a POSITA would have understood that causing Salmela's device 10 to present notifications at different points in Salmela's process to update subscription credentials 26 would have been beneficial to assure the user of device 10 that the device is operating as intended. EX1003, ¶68. A POSITA would have also understood that causing Salmela's device 10 to present notifications at different points in the process to update subscription credentials 26 would have been useful to provide the user with information concerning a process for connecting to the wireless access network. EX1003, ¶69.

Implementing Salmela's device to present notifications at different points in the process to update subscription credentials 26 as suggested by Sigmund would have been obvious as a predictable application of a known technique (e.g., presenting notifications) to Salmela's known system to achieve merely predictable results. *KSR*, 550 U.S. at 417 (2007); EX1003, ¶70. Considering the predictable electrical/network and software components involved in the combination and the relatively advanced state of the art at the time, a POSITA would have reasonably

expected success achieving the combination before the earliest effective filing date of the '510 Patent (Mar. 14, 2013). EX1003, ¶71.

3. *Application to Challenged Claims*

Claims [4], [5], [8], [9], [10]

Sigmund discloses a mobile device that, like device 10 of the Salmela-Rishy-Maharaj combination, accesses a wireless access network to receive one or more services. EX1008, [0024]-[0031]; EX1003, ¶222; *supra* §V.E.1. Sigmund also discloses a “process...for handling a password reset request” from a user, the process notifying the user of various information including whether the reset request is successful or unsuccessful. EX1008, [0032]-[0040], FIGS. 2-3; *supra* §V.E.1. As described above, it would have been obvious based on Sigmund to cause notifications to be presented through a user interface (e.g., a display) of Salmela’s device 10 in response to various events in Salmela’s process for updating credentials. *Supra*, §V.E.1; EX1003, ¶222.

A POSITA would have known that notifications were commonly employed by the Critical Date of the '510 Patent to inform mobile device users about a wide range of events, including to report the status or results of processes performed on the mobile device. EX1008, [0036] (“A visual prompt can be presented to the subscriber as a cue or reminder ...”); EX1003, ¶223. In this context, it would have been obvious to cause Salmela’s device 10 to present notifications to the user at

any point during the credential updating process—including in response to determining that the updated subscription credential does or does not match the target credential (and indeed anytime the device 10 performs the comparison between current and expected credentials as described at paras. [0041] and [0044] of Salmela). EX1004, [0041], [0044]; *supra*, Ground 1A at [2], [7]; EX1003, ¶223. The fact that displaying notifications by wireless devices was well-known by 2013 is corroborated by numerous references. EX1003, ¶223 (citing corroborating EX1020, 29; EX1021, 26; EX1022, FIGS. 2A-2D; EX1023, FIGS. 4-8). In the combination, for example, Rishy-Maharaj confirms that the user interface of the wireless device is configurable to present notifications to the user during a credential updating process. EX1005, [0168] (“The display 702 is a component configured to show images and notifications in order to allow a user to understand the state of the wireless device ...”), [0130] (“wireless device 102 [is] notified that the subscription has been created ... and wireless device 102 prepare[s] to receive the credentials”).

From a POSITA’s general knowledge of well-known notification technology developed before the Critical Date of the ’510 Patent, as evidenced by Sigmund and other prior art references, a POSITA would have presented notifications based on the results of this matching operation, for example, to inform the user whether the device 10 has detected that new subscription credentials are available, that the

device 10 is in the process of obtaining new subscription credentials if available, and whether an error has been detected. EX1003, ¶224. A POSITA would have expected users to find this information helpful since it would help the user better understand if his or her earlier request to update the subscription plan for the device 10 had been effected and whether device 10's failure to gain network access was related to the user's request or if it stemmed from a different problem, for example. EX1003, ¶224.

Claims [4], [5], [8], [9], and [10] each refer to notifications presented through the user interface of the device that report different content to the user. EX1003, ¶225. These limitations amount to no more than printed matter, however, and are not entitled to patentable weight. The Federal Circuit has held that limitations such as these, which have no functional or structural relationship to the device or substrate on which the information is disposed, "will not distinguish the invention from the prior art in terms of patentability." *In re Gulack*, 703 F. 2d 1381, 1385 (Fed. Cir. 1983); *see, e.g., In re DiStefano*, 808 F. 3d 845, 848-851 (Fed. Cir. 2015).

Even if the contents of the notifications described in these claims were entitled to patentable weight (which they are not), they would have been obvious to a POSITA for the reasons described above. EX1003, ¶226. For example, it would have been obvious to report an error as recited in claim [4] when the updated and

target subscription credentials do not match to inform the user of the need for a new credential or that a credential has been corrupted—especially since error reports were common before the alleged invention of the '510 Patent. *Supra*, Ground 2A at [2]. It would have been obvious to report that a credential update is in progress as recited in claim [5] when the updated and target credential do not match to inform the user that the device 10 is taking action to update the subscription and resolve the issue that led the device to fail to gain network access. EX1008, [0034]. It would have been obvious to report that the particular credential has been replaced by the target credential as recited in claim [8] when the updated and target credential do match to assure the user that no new subscription credentials are necessary at the current time since the subscription credentials were already updated successfully. EX1003, ¶226; *supra*, Ground 2A at [7].

It would have been obvious to report a status of the user request to replace the particular subscription credential with the target credential as recited in claim [9] to keep the user apprised of the status of the device's attempts to acquire new subscription credentials. EX1003, ¶227. Finally, it would have been obvious to request confirmation of the user request to replace the particular credential with the target credential as recited in claim [10] to ensure the user intended to make the request and to provide the user with an opportunity to cancel the request if it was

initially mistakenly submitted. EX1003, ¶227 (citing corroborating EX1023, FIG. 4, EX1024, FIG. 4).

F. GROUND 1F: Salmela, in view of Rishy-Maharaj, and further in view of Johansson would have rendered obvious claim 40

1. *Johansson*

Johansson describes a wireless device (e.g., user equipment) configured to receive temporary network access credentials such as a temporal mobile station identifier (TMSI) from a remote connectivity providing unit. EX1009, [0047]-[0049], [0050]-[0056], FIGS. 2-3; EX1003, ¶72-73.

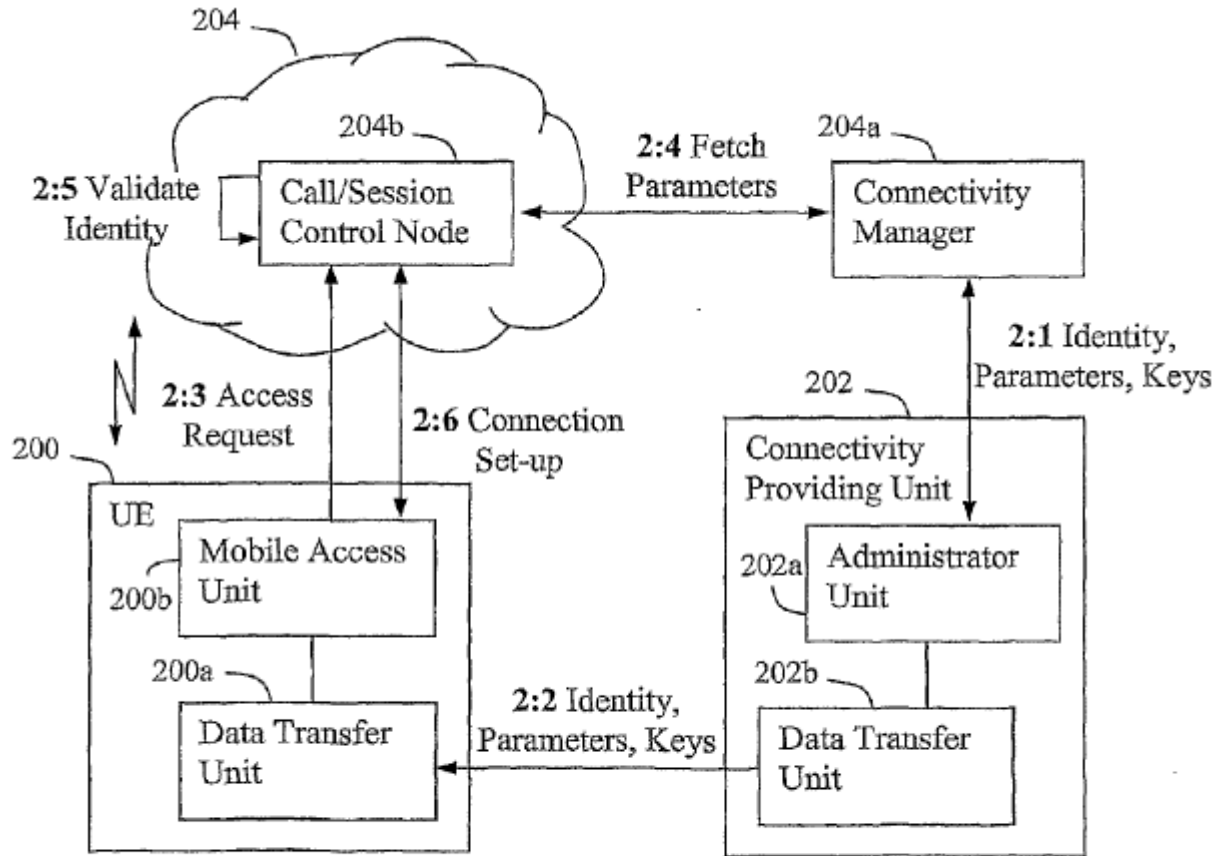


Fig. 2

EX1009, FIG. 2

2. *The Salmela-Rishy-Maharaj-Johansson Combination*

To the extent Salmela does not disclose in detail how the temporary access credentials 30 may be loaded on device 10 during its initial configuration or in other suitable manners, Johansson discloses the conventional option of obtaining temporary access credentials from a network system communicatively coupled to a wireless device. *Supra*, §V.F.1; EX1003, ¶¶74-75. Multiple reasons would have

prompted a POSITA to implement Salmela's device 10 in accordance with Johansson's suggestions for obtaining temporary access credentials from a network system before the Critical Date of the '510 Patent. EX1003, ¶75-79.

Obtaining temporary access credentials from a network system as suggested by Johansson, for example, would have been obvious and beneficial to allow device 10 to achieve temporary access in cases where device 10 was not pre-provisioned with the correct temporary access credentials during manufacture of the device 10. EX1003, ¶76. A POSITA would have also understood that allowing device 10 to receive temporary credentials from a network element would be beneficial when a service provider seeks to strictly control temporary access to the service provider network by declining to pre-provision wireless devices with credentials. EX1003, ¶77. Furthermore, obtaining temporary access credentials from a network system as suggested by Johansson would have been obvious as a predictable application of Johansson's known technique to Salmela's known system to achieve merely predictable results. *KSR*, 550 U.S. at 417; EX1003, ¶78. Considering the predictable electrical/network and software components involved in the combination and the relatively advanced state of the art at the time, a POSITA would have reasonably expected success achieving the combination before the Critical Date. EX1003, ¶79.

3. *Application to Challenged Claims*

Claim [40]

Johansson discloses techniques for using a mobile station to obtain a ***temporary credential*** from a ***network system*** communicatively coupled to the mobile station. EX1009, [0045]-[0052], FIG. 2; *supra*, §V.F.1; EX1003, ¶228. For example, Johansson discloses that a connectivity providing unit 202 acquires a temporary connectivity identity (e.g., TMSI) and “pushes” this temporary connectivity identity to user equipment 200. EX1009, [0047]-[0048]. Connectivity providing unit 202 of Johansson represents a ***network system*** that is separate from the user equipment, which represents a ***wireless device***:

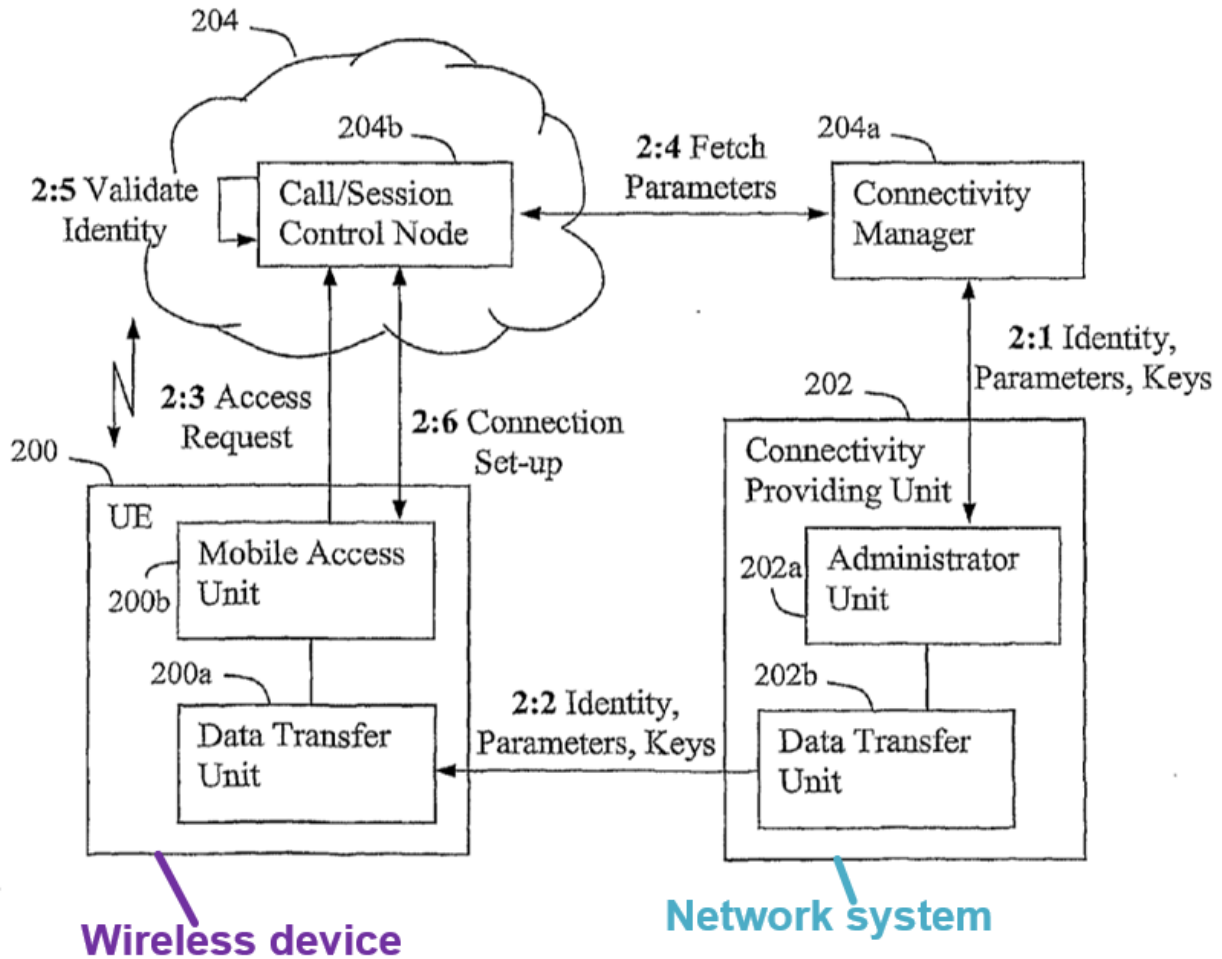


Fig. 2

EX1009, FIG. 2 (annotated).

Johansson thus discloses that the user equipment obtains the temporary credential from the connectivity providing unit communicatively coupled to the user equipment. EX1003, ¶229. As discussed above, it would have been obvious and a POSITA would have been motivated to implement device 10 according to Johansson's teachings such that it would obtain temporary access credentials 30 from a network system communicatively coupled to device 10. EX1003, ¶229; *supra* §V.F.2.

G. GROUND 1G: Salmela, in view of Rishy-Maharaj, and further in view of Slavov would have rendered obvious claim 34

1. *Slavov*

Slavov describes a process by which a user subscribes a wireless device 100 to a home network 20 through a web interface or website. EX1011, [0024], [0049]; *see also id.*, [0005]-[0007], [0023], [0026]-[0028], FIGS. 1-2; EX1003, ¶80-82.

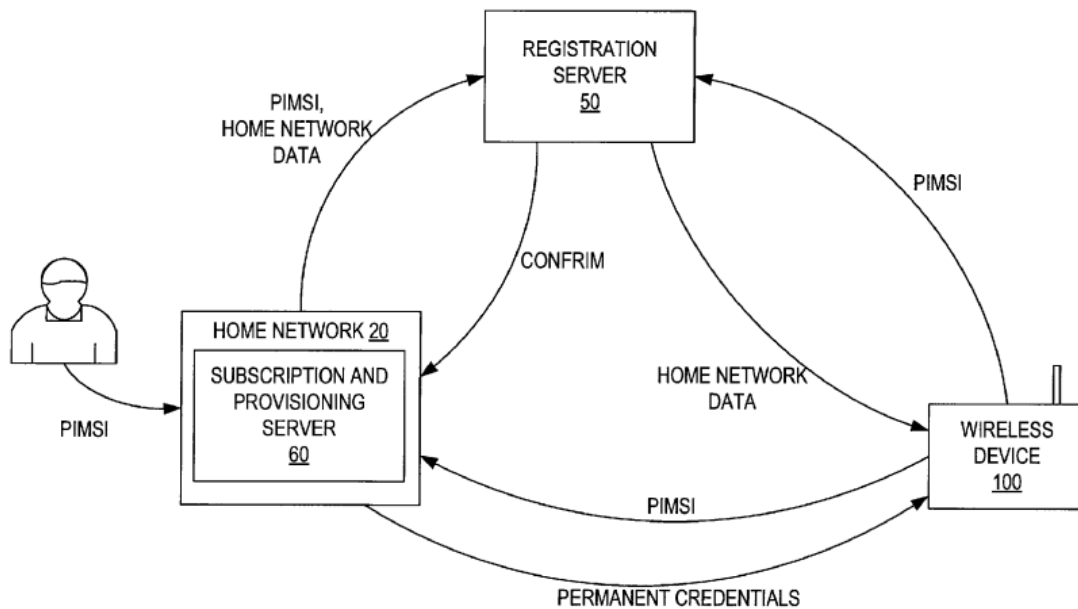


FIG. 2

EX1011, FIG. 2.

2. *The Salmela-Rishy-Maharaj-Slavov Combination*

To the extent Salmela and Rishy-Maharaj do not expressly disclose that device 10 obtains information through a website as part of receiving a user request through a user interface, Slavov provides this feature. EX1011, [0024], [0049];

EX1003, ¶83. Multiple reasons would have prompted a POSITA to implement device 10 of the Salmela-Rishy-Maharaj combination in accordance with Slavov's suggested technique for a user indicate a selected subscription plan through a website before the alleged invention of the '510 Patent. EX1003, ¶83. For example, in the combination, the user interface described in Rishy-Maharaj could predictably be a web-based interface with information about available subscription plans received from a website and presented on the device 10 through a web browser or other web portal or application. EX1005, [0111], [0112]; EX1003, ¶83.

For example, implementing device 10 according to Slavov's suggestion for permitting a user to subscribe to wireless services through a website would have advantageously allowed the user to subscribe to a new plan and request new subscription credentials through a standard web browser or other application on the device capable of loading a website. EX1003, ¶84. Implementing device 10 according to Slavov's suggestion for permitting a user to subscribe to wireless services through a website would predictably guide the user to provide inputs through the user interface of device 10. EX1003, ¶85. Furthermore, implementing device 10 of the Salmela-Rishy-Maharaj combination so that a user can interact with device 10 through a website as suggested by Slavov would have been obvious as a predictable application of a known technique (e.g., using a website to subscribe to a home network) to a known system to achieve merely predictable

results, and would have been obvious to try as one of a finite number of ways to receive user input. *KSR*, 550 U.S. at 417; EX1003, ¶86.

A POSITA also would have reasonably expected success implementing the Salmela-Rishy-Maharaj-Slavov combination. EX1003, ¶87. Indeed, wireless devices of the same or similar types as those described in the Salmela-Rishy-Maharaj combination permit internet browsing of websites. *See, e.g.*, EX1004, [0021] (“device 10 is a cellular communication device, such as a cellular radiotelephone, pager, PDA, computer or network access card”); EX1005, [0030] (“wireless device 102 may be any wireless electronic device capable of connecting to a network, such as a phone, personal desktop assistant (‘PDA’), laptop computer, tablet, or netbook, for example”). Wireless devices by the Critical Date of the ’510 Patent (e.g., March 14, 2013) commonly included interfaces, applications, network connectivity, internet browsing, and other capabilities sufficient to provide a website for prompting user input as taught in Slavov. EX1003, ¶87.

3. *Application to Challenged Claims*

Claim [34]

Slavov describes a wireless device 100 that can use a temporary device identifier (e.g., a preliminary international mobile subscriber identity (PIMSI)) to automatically obtain permanent subscription credentials for accessing a home

network 20. EX1011, [0022]-[0028], [0049], FIGS. 1-2, 10. Before the wireless device 100 contacts home network 20 using the temporary device identifier, a user can subscribe wireless device 100 to home network 20 through a website. EX1011, [0049] (“The subscription and provisioning server 60 may provide a website accessible to device owners for subscribing to the services of the home network 20.”), [0024]. The wireless device receives information about available subscriptions that the user can select, as described in Rishy-Maharaj, which can be obtained from a website, as described in Slavov. *Id.*; *see also id.*, EX1005, [0110]-[0111]. As described in the preceding section (§V.G.2), it would have been obvious to apply Slavov’s suggested use of a website as a web interface through which a user can provide inputs on Salmela’s device 10 to subscribe to a new home network to the Salmela-Rishy-Maharaj combination (e.g., using a web browser or similar web portal on device 10). *Supra*, §V.G.2. In the resulting Salmela-Rishy-Maharaj-Slavov combination, the device 10 would obtain the user request to replace the current subscription credential 26 (e.g., the particular credential) with the target credential by obtaining information about available subscriptions and the user’s selection from a website based on the teachings of Slavov. *Supra*, Element [1f]; EX1003, ¶230.

H. GROUND 1H: Salmela, in view of Rishy-Maharaj, and further in view of Gupta would have rendered obvious claim 44

1. *Gupta*

Gupta discloses a wireless communication device 120 that can make a voice call as part of a “staging process” to prepare the device for operating in the wireless network. EX1013, [0017]-[0021], [0023]-[0043], FIGS. 1-2; EX1003, ¶88-89.

2. *The Salmela-Rishy-Maharaj-Gupta Combination*

To the extent that Salmela does not expressly disclose that device 10 initiates the programming session by communicating with the network element through a voice call, Gupta discloses the conventional option of a wireless device staging (e.g., authenticating) with a network element by making a voice call. EX1013, [0021], [0034]-[0043], FIG. 2, *supra*, §V.H.1. Multiple reasons would have prompted a POSITA to implement Salmela’s device 10 in accordance with Gupta’s suggestions for a wireless device to initiate a programming session by making a voice call before the Critical Date of the ’510 Patent. EX1003, ¶90-94.

For example, implementing device 10 of the Salmela-Rishy-Maharaj combination to initiate a programming session by making a voice call as suggested by Gupta would beneficially allow device 10 to automatically be provisioned when the user makes a call. EX1003, ¶91. Additionally, a POSITA would have

understood that allowing device 10 to initiate a programming session by making a voice call as suggested by Gupta would cause device 10 to initiate a programming session with a network element in a situation where a network-provisioning state change becomes apparent. EX1003, ¶92. Initiating a programming session through making a voice call as taught by Gupta would have been obvious as a predictable application of Gupta's known technique to a known system as taught by Salmela to achieve merely predictable results. *KSR*, 550 U.S. at 417; EX1003, ¶93.

Considering the predictable electrical/network and software components involved in the combination and the relatively advanced state of the art at the time, a POSITA would have reasonably expected success achieving the combination before the Critical Date. EX1003, ¶94.

3. *Application to Challenged Claims*

Claim [44]

Gupta discloses that a **wireless device** (e.g., wireless communication device 120) can communicate with a wireless communication station 130 via radiofrequency (RF) signals by making a **voice call**. EX1013, [0017], [0021], [0034]-[0037], [0044]-[0051], FIG. 2, FIG. 3; EX1003, ¶231. This **voice call** can be received by a **network element** (e.g., network infrastructure 140) through the wireless communication station 130. EX1013, [0034]-[0037], FIG. 2. Based on receiving the **voice call**, the network infrastructure 140 can authenticate the

wireless communication device 120 and send “encrypted staging data” to wireless communication device 120. EX1013, [0036], [0037], FIG. 2. Thus, the *voice call* placed by Gupta’s *wireless device initiates a programming session* with a *network element* that results in the device being provisioned with “encrypted staging data.” EX1013, [0036], [0037], FIG. 2. In the predictable Salmela-Rishy-Maharaj-Gupta combination, device 10 would therefore place a *voice call* to *initiate a programming session* with Salmela’s credentials server in a way that causes device 10 to be provisioned with new subscription credentials. EX1013, [0017], [0021], [0034]-[0037], FIG. 2, *supra*, §V.H.2.

VI. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION

A. Discretionary denial under §325(d) is not warranted

This Petition does not present a situation where “the same or substantially the same prior art or arguments” were previously considered by the Office to warrant denial under § 325(d). *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 (Feb. 13, 2020 (Precedential)). Although Salmela was cited in an IDS during prosecution as one of more than *1,500 references* listed on the face of the patent, Salmela was never substantively addressed in any office action or remarks in connection with original examination of the ’510 patent. EX1001, Cover; EX1002; *supra*, §II.B. Rishy-Maharaj was never cited at all, and thus never considered in combination with

Salmela. Nor were Bennett, Ionescu, Sigmund, Johansson, Slavov, FCCReg, or Gupta discussed on the record during prosecution. *Id.* For this reason alone, such “new, noncumulative prior art asserted in the Petition” weighs against discretionary denial. *Oticon Medical AB v. Cochlear Ltd.*, IPR2019-00975, Paper 15 at 20 (Oct. 16, 2019 (§§II.B and II.C precedential)). Even if the Examiner had considered any prior art containing teachings cumulative to the teachings of the references cited in this Petition, allowing the ’510 Patent over such teachings/prior art amounts to material error in light of the relevance of those teachings to the Challenged Claims as demonstrated herein. These circumstances all counsel against denial under §325(d).

B. Discretionary denial under §314(a) is not warranted

This Petition’s merits are compelling, and the evidence presented herein is substantial, counseling against discretionary denial under *Fintiv*. SAMSUNG-1101 4-5. Moreover, the *Fintiv* factors counsel against denial.

Factor 1 is neutral because neither party has requested a stay in the co-pending litigation.

Factor 2 is neutral because the Court’s trial date is speculative and subject to change. The Board will likely issue its Final Written Decision around August 2026, approximately six months after the currently scheduled trial date (February

9, 2026). EX1102, 1. However, as the Board/Director have recognized, “scheduled trial dates are unreliable and often change.” EX1101, 8.

Factor 3 favors institution because Petitioner has diligently filed this Petition months ahead of the one-year time bar, while the co-pending litigation in E.D. Tex. is in its early stages. Beyond exchanging preliminary infringement and invalidity contentions, the parties and the court have yet to expend significant resources on invalidity. EX1102. By the anticipated institution deadline in August 2025, the co-pending litigation will still be in early stages—fact and expert discovery will be ongoing, and the *Markman* hearing will not have occurred. *Id.*

Factor 4 favors institution because Petitioner stipulates to not pursuing the IPR grounds in the co-pending litigation. EX1026. Thus, institution serves “efficiency and integrity goals” by “not duplicating efforts” and “resolving materially different patentability issues.” *Apple, Inc. v. SEVEN Networks, LLC*, IPR2020-00156, Paper 10, 19 (June 15, 2020); *Sand Revolution II, LLC v. Continental Intermodal Group-Trucking LLC*, IPR2019-01393, Paper 24, 12 (June 16, 2020); *Google LLC v. Flypsi, Inc.*, IPR2023-00360, Paper 9, 36-39 (August 2, 2023).

Factor 5 is neutral. The same parties are in the co-pending litigation.

Factor 6 favors institution because this Petition’s merits are compelling, as described herein.

VII. CONCLUSION AND FEES

The Challenged Claims are unpatentable. Petitioner authorizes charge of fees to Deposit Account 06-1050.

VIII. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1)

A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, “Samsung”) are the real parties-in-interest. No other party had access or control over this Petition, and no other party provided funding for this Petition.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The '510 Patent is the subject of a civil action in *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al*, 2-24-cv-00228 (E.D. Tex.), filed April 3, 2024 (EX1100).

Petitioner is concurrently filing a separate IPR petition challenging the '510 Patent in IPR2025-00483.

Petitioner is not aware of any other disclaimers or reexamination certificates addressing the '510 Patent.

Attorney Docket No. 39843-0183IP2
IPR of U.S. Patent No. 9,609,510

C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Petitioner provides the following designation of counsel.

Lead Counsel	Backup counsel
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email: IPR39843-0183IP2@fr.com	Jeremy J. Monaldo, Reg. No. 58,680 Nicholas Stephens, Reg. No. 74,320 Cameron A. Ubel, Reg. No. 77,081 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 PTABInbound@fr.com

D. Service Information

Please address all correspondence and service to the address listed above.

Petitioner consents to electronic service by email at IPR39843-0183IP2@fr.com

(referencing No. 39843-0183IP2 and cc'ing PTABInbound@fr.com, axf-ptab@fr.com, monaldo@fr.com, nstephens@fr.com, and ubel@fr.com).

Respectfully submitted,

Dated 02/10/2025

/Nicholas W. Stephens/

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Nicholas Stephens, Reg. No. 74,320
Cameron A. Ubel, Reg. No. 77,081
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2025-00484)

Attorneys for Petitioner

Attorney Docket No. 39843-0183IP2
IPR of U.S. Patent No. 9,609,510

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 13,818 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated 02/10/2025

/Nicholas W. Stephens/
W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Nicholas Stephens, Reg. No. 74,320
Cameron A. Ubel, Reg. No. 77,081
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on February 10, 2025, a complete and entire copy of this Petition for *Inter Partes* Review, Notice Ranking Petitions, Power of Attorney and all supporting exhibits were provided by Federal Express, to the Patent Owner, by serving the correspondence address of record as follows:

Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

/Diana Bradley/
Diana Bradley
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(858) 678-5667